Australian Government

Australian Law Reform Commission

For Your Information

REPORT

Australian Privacy Law and Practice

Volume 3
REPORT 108
May 2008

This Report reflects the law, and the policies of federal bodies, as at 31 March 2008.

ISBN: 978-0-9804153-2-2

Commission Reference: ALRC 108 (Final Report)

The Australian Law Reform Commission was established on 1 January 1975 by the *Law Reform Commission Act 1973* (Cth) and reconstituted by the *Australian Law Reform Commission Act 199*6 (Cth). The office of the ALRC is at Level 25, 135 King Street, Sydney, NSW, 2000, Australia.

All ALRC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the ALRC.

Telephone:	within Australia	(02)	8238 6333
	International	+61 2	8238 6333
TTY:		(02)	8238 6379
Facsimile:	within Australia	(02)	8238 6363
	International	+61 2	8238 6363

E-mail: info@alrc.gov.au

ALRC homepage: www.alrc.gov.au

Printed by Paragon Group

Summary of Contents

Volume 1

Volume 2

Part G

Credit Reporting Provisions

52. Overview: Credit Reporting

Contents

Introduction

52.1 The *Privacy Amendment Act 1990* (Cth), which commenced operation in September 1991, extended the coverage of the *Privacy Act* to consumer credit reporting. The credit reporting provisions of the *Privacy Act 1988* (Cth) are contained in Part IIIA and associated provisions (the credit reporting provisions).[1]

52.2 The credit reporting provisions regulate the collection, use and disclosure of personal information concerning credit that is intended to be used wholly or primarily for domestic, family or household purposes.[2] Commercial credit information is only incidentally regulated by the Act, for example, where it is used to assess an application for consumer credit.[3]

52.3 In Part G, the ALRC examines the credit reporting provisions and makes recommendations for reform. This chapter introduces the topic by describing the role of credit reporting, the background to the national regulation of credit reporting through the *Privacy Act*, and the legislative history of the credit reporting provisions.

---

1 The major associated provisions include definitions and interpretation provisions: *Privacy Act 1988* (Cth) ss 6, 11A, 11B; and provisions dealing with the *Credit Reporting Code of Conduct*: ss 18A, 18B.

2 See the definitions of 'commercial credit' and 'credit': Ibid s 6(1).

3 Ibid s 18L(4).

52.4 In Chapter 53, the ALRC provides a summary of the content of the credit reporting provisions, the responsibilities and powers of the Office of the Privacy Commissioner (OPC) with regard to credit reporting,[4] and the remedies and penalties available in the event of non-compliance with the credit reporting provisions.[5]

52.5 In Chapter 54, the ALRC introduces its approach to reform of the credit reporting provisions. The ALRC recommends that the credit reporting provisions be repealed and credit reporting regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles (UPPs),[6] and regulations under the *Privacy Act*—referred to in this Report as the new *Privacy (Credit Reporting Information) Regulations*—which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information. The ALRC also makes a range of other recommendations concerning the general approach to the drafting and application of the regulations. Finally, it recommends that a credit reporting code providing detailed guidance within the framework provided by the Act and regulations be developed by credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the OPC.

52.6 In Chapter 55, the ALRC considers extending the current system of credit reporting to permit a broader spectrum of personal information to be collected and disclosed—referred to in this Report as 'more comprehensive' credit reporting. The ALRC examines the arguments for and against more comprehensive credit reporting, with particular reference to comments received in submissions and consultations, and information derived from empirical research into the possible effects of more comprehensive credit reporting on credit markets and the economy. The ALRC recommends an extension in the categories of personal information that may be collected for credit reporting purposes—including to repayment performance history information subject to there being an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

52.7 The collection of credit reporting information, the permitted content of credit reporting information and notification of collection are discussed in Chapter 56. The ALRC makes a range of recommendations in relation to, among other things, regulating the collection of information about small overdue payments, dishonoured cheques, personal insolvency, serious credit infringements and debts of children and young people. The ALRC also recommends new notification requirements.

52.8 Issues concerning the use and disclosure of credit reporting information are discussed in Chapter 57. The ALRC makes a range of recommendations concerning the relationship between the 'Use and Disclosure' principle in the model UPPs and the new *Privacy (Credit Reporting Information) Regulations*, and the regulation of the use

4 The powers and responsibilities of the OPC generally are discussed in Part F.
5 The remedies and penalties available under the Act generally are discussed in Part F.
6 As discussed in Part D.

and disclosure of credit reporting information in specific contexts. These contexts include mortgage and trade insurance, debt collection, direct marketing and identity verification.

52.9 In Chapter 58, the ALRC discusses the quality and security of credit reporting information. The ALRC makes a range of recommendations in relation to regulating the reporting of statute-barred debts, overdue payments, and schemes of arrangement, and to improving data quality generally. The deletion of credit reporting information after maximum permitted periods of retention and data security are also discussed.

52.10 Individual rights of access to, and correction of, credit reporting information are discussed in Chapter 59. How these matters should be dealt with under the model UPPs and new *Privacy (Credit Reporting Information) Regulations* are set out in the recommendations. The ALRC examines complaint handling in credit reporting disputes by the OPC and other complaint-handling mechanisms, and penalties for breach of the regulations. Importantly, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should provide that credit providers only may list overdue payment or repayment performance history where the credit provider is a member of an external dispute resolution scheme recognised by the OPC.

What is credit reporting?

52.11 Credit reporting involves providing information about an individual's credit worthiness to banks, finance companies and other credit providers, such as retail businesses that issue credit cards or allow individuals to have goods or services on credit. Credit reporting is generally conducted by specialised credit reporting agencies that collect and disclose information about potential borrowers, usually in order to assist credit providers to assess applications for credit.

52.12 Credit reporting agencies collect information about individuals from credit providers and publicly available information (such as bankruptcy information obtained from the Insolvency and Trustee Service Australia—a federal government agency). This information is stored in central databases for use in generating credit reporting information for credit providers. In assessing credit applications, this information augments information obtained directly from an individual's application form and the credit provider's own records of past transactions involving the individual.

52.13 Credit reporting agencies also provide information processing services that assist credit providers to assess credit applications. One agency, Veda Advantage, stated that:

> Statistical modelling of individuals' behaviour over significant timeframes has enabled Veda Advantage to provide its customer base with the credit file characteristics which are statistically relevant to the probability of default.

> Customisation of these credit file and behavioural characteristics by each subscriber is based on the particular risk model, portfolio and competitive positioning.[7]

52.14 The information contained in credit reporting databases may be used in credit scoring systems. Credit scoring may be described as the use of 'mathematical algorithms or statistical programmes that determine the probable repayments of debts by consumers, thus assigning a score to an individual based on the information processed from a number of data sources'.[8] In Australia, credit scoring systems used by individual credit providers are often referred to as 'scorecards'.

52.15 As Professor Daniel Solove explains, credit reporting is an understandable response to a modern, interconnected world containing 'billions of people' and where 'word-of-mouth is insufficient to assess reputation'. He goes on to state:

> Credit reporting allows creditors to assess people's financial reputations in a world where first-hand experience of the financial condition and trustworthiness of individuals is often lacking.[9]

52.16 The role of a credit reporting agency is to provide rapid access to accurate and reliable standardised information on potential borrowers. Such information enables credit providers to manage the risks of lending and to guard against identity fraud. Economic theorists note that:

> Credit reporting addresses a fundamental problem of credit markets: asymmetrical information between borrowers and lenders that leads to adverse selection and moral hazard.[10]

52.17 Information asymmetry refers to the fact that, because a credit provider often cannot know the full extent of an applicant individual's credit history, the individual has more information about his or her credit risk than the credit provider. Adverse selection arises where a credit provider, operating in response to information asymmetry, prices credit based on the *average* credit risk of individuals. This creates an incentive for high risk applicants to apply (the price is low to them) and low risk applicants to reject credit (it is overpriced for them).

> The result is adverse selection because the client group the credit provider ends up with is a higher risk than the credit provider priced for. Better information allows credit providers to more accurately measure borrower risk and set loan terms accordingly, which is why credit providers maintain their own databases of information on a consumer but also seek out information shared by other credit providers and supplied to them by a credit reporting agency.[11]

---

7 Veda Advantage, *Submission PR 272*, 29 March 2007.

8 F Ferretti, 'Re-thinking the Regulatory Environment of Credit Reporting: Could Legislation Stem Privacy and Discrimination Concerns' (2006) 14 *Journal of Financial Regulation and Compliance* 254, 261.

9 D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 507–508.

10 M Miller, 'Introduction' in M Miller (ed) *Credit Reporting Systems and the International Economy* (2003) 1, 1.

11 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 247.

52.18 Information asymmetry also creates a moral hazard. A credit applicant may obtain credit fraudulently by failing to disclose his or her credit history. Credit reporting reduces such moral hazard because non-payment to one credit provider can inform the actions of other credit providers.[12]

52.19 While the major purpose of credit reporting is to provide information to assist credit providers to assess applications for credit, credit reporting also may be seen as serving the associated purpose of facilitating responsible lending. That is, the information provided by credit reporting to credit providers may help to prevent individuals becoming financially overcommitted. Credit reporting also assists in trade and mortgage insurance, and in debt collection.

Credit reporting agencies

52.20 At present, there are three main credit reporting agencies operating in the Australian market. These are—in order of market share—Veda Advantage, Dun and Bradstreet and the Tasmanian Collection Service.

52.21 The major consumer credit reporting agency is Veda Advantage (previously named Baycorp Advantage), which states that it maintains credit worthiness related data on more than 11 million individuals in Australia and New Zealand.[13] It has over 5,000 subscribers from a wide range of industries, including banking, finance telecommunications, retail, utilities, trade credit, government, credit unions and mortgage lenders.[14]

52.22 Veda Advantage's Australian credit reporting business commenced in 1968 as the Credit Reference Association of Australia (CRAA), which was established by the finance industry.[15] As discussed below, the CRAA played a central role in developments leading to the enactment of the credit reporting provisions of the *Privacy Act*.[16]

---

12 M Miller, 'Introduction' in M Miller (ed) *Credit Reporting Systems and the International Economy* (2003) 1, 1.

13 Veda Advantage, *Frequently Asked Questions—Who is Veda Advantage?* (2007) <www.mycreditfile.com.au> at 11April 2008.

14 Veda Advantage, *Submission PR 163*, 31 January 2007.

15 Veda Advantage, *Frequently Asked Questions—Who is Veda Advantage?* (2007) <www.mycreditfile.com.au> at 11April 2008.

16 The following background to the enactment of the *Privacy Act* credit reporting provisions is drawn primarily from an article prepared by Roger Clarke, then chair of the Economic, Legal and Social Implications Committee of the Australian Computer Society: R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society; and from annual reports of the New South Wales Privacy Committee: New South Wales Government Privacy Committee, *Annual Report 1984* (1984); New South Wales Government Privacy Committee, *Annual Report* (1989).

Background to national regulation

52.23 There is an almost universal view that the practice of credit reporting should be regulated. There are many reasons for this. One is that it vindicates an individual's right to privacy—as Professor Solove puts it, '[p]eople expect certain limits on what is known about them and on what others will find out'.[17] Another justification is that a credit report, which contains aggregated personal information, can be used to make decisions that 'profoundly affect a person's life'.[18] As such, there is special urgency in ensuring that such information is accurate and not misused.

State legislation

52.24 The first Australian legislation regulating aspects of credit reporting was enacted in 1971. In Queensland, Part III Division I of the *Invasion of Privacy Act 1971* (Qld) established a licensing scheme for credit reporting agents. The Act included statutory provisions dealing with the:

- permitted purposes of credit reports;
- information to be furnished to consumers and credit reporting agencies when credit is refused on the basis of a credit report;
- information to be disclosed by credit reporting agencies on request by consumers; and
- obligations on credit reporting agencies to investigate and correct inaccurate information and delete old information.[19]

52.25 The *Invasion of Privacy Act* contained offences in relation to: obtaining information falsely from a credit reporting agency; unauthorised disclosure of credit reporting information; supplying false credit reporting information; and demanding payment by making threats in relation to credit-related information.[20] The credit reporting provisions of the Act were repealed in 2002.[21]

52.26 In 1975, South Australia enacted the *Fair Credit Reports Act 1975* (SA), which provided individuals with rights of access to, and correction of, information in consumer reports; required credit reporting agencies to adopt procedures to ensure the accuracy and fairness of consumer reports; and required traders to inform individuals of their use of adverse information in such reports.[22] The Act was repealed in 1987.[23]

---

17 D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 508.
18 Ibid, 508.
19 *Invasion of Privacy Act 1971* (Qld) ss 16, 17, 18, 24.
20 Ibid ss 19, 20, 21, 22, 25.
21 *Tourism, Racing and Fair Trading (Miscellaneous Provisions) Act 2002* (Qld) s 45.
22 *Fair Credit Reports Act 1975* (SA) pt II.
23 *Statutes Amendment (Fair Trading) Act 1987* (SA) s 16.

52.27 In Victoria, the *Credit Reporting Act 1978* (Vic) provides consumers with rights of access to copies of files held in relation to them by a credit reporting agency and provides a mechanism to dispute details and request the amendment of incorrect information. Credit reporting regulations were made in 1978 to prescribe procedures and time limitations to be followed by consumers seeking to amend personal credit reports held by credit agents.[24] The Victorian Consumer Credit Review noted that:

> With the commencement of the [federal] *Privacy Act*, however, it appears that the continuing relevance of the Victorian Act declined because the *Privacy Act* was binding on the industry and more comprehensive for consumers.[25]

52.28 Australia's first privacy regulator, the New South Wales Privacy Committee, identified credit reporting as an important privacy issue.[26] In 1976, concerns about the privacy of credit reporting information led the Privacy Committee and the CRAA to enter a so-called 'Voluntary Agreement' under which the CRAA would provide individuals with access to the information it held about them.[27]

52.29 Despite the Voluntary Agreement, few incentives existed to encourage CRAA's credit provider subscribers to comply with the Voluntary Agreement, notify individuals about adverse reports and rights of access, or to ensure that information they provided to the CRAA was accurate and complete.[28] Some observers expressed serious doubts about the willingness and ability of the CRAA to discipline its member credit providers.

> Few clients appear to have ever been suspended, had their memberships cancelled, or had specific employees suspended, for breach of CRAA rules. In 1985, when the Secretary of a Hibernian Credit Union was found to have made an enquiry for purposes other than credit granting (and in the process invented an application for a $50,000 mortgage loan), CRAA failed to discipline either its client or the client's employee (NSW Privacy Committee Annual Report, 1985, 92–98). Even a Report to Parliament, the NSW Privacy Committee's ultimate sanction, had no effect.[29]

52.30 During 1983, the New South Wales Privacy Committee reviewed its experience with the Voluntary Agreement and concluded that self-regulation of the credit reporting industry was ineffective. The Committee made proposals that it hoped would be the basis of fair credit reporting legislation or a code of practice under consumer

---

24 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 266.
25 Ibid, 266.
26 Established under the *Privacy Committee Act 1975* (NSW).
27 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 4.
28 Ibid, 4–5.
29 Ibid, 5.

protection legislation.[30] The Committee stated that this position was in line with its view that the 'time is now ripe for information privacy legislation'.[31]

52.31 In 1989, one commentator on privacy issues stated:

> Judging by the last decade's complaints and enquiries to the country's only long-standing privacy 'watchdog', the NSW Privacy Committee, the public regards consumer credit reporting as the largest single information privacy issue.[32]

New regulatory momentum

52.32 The momentum for regulation of credit reporting intensified in the late 1980s. In large part this was in response to proposals by the CRAA to implement a new system of credit reporting. This system was referred to by the CRAA as the Payment Performance System (PPS) and was described by the CRAA and others as a form of 'positive' reporting.[33]

52.33 In the 1980s, credit reporting in Australia did not involve the collection or disclosure in credit reports of so-called 'positive' information about an individual's credit position. Apart from publicly available information about bankruptcies and court judgments, credit information was restricted to default reports made by CRAA members—that is, 'negative' information.

52.34 During the latter part of 1988, CRAA publicised an intention to augment its collection of credit reporting information by including information about individuals' current credit commitments. The nature of the proposal was summarised by Clarke as follows:

> Under PPS, credit providers would supply CRAA with tapes containing their customers' credit accounts. This data would be merged with previously recorded data every 30 to 60 days. Reports would then contain a complete listing of all known credit accounts, balances owing (at some recent point in time), and the consumer's payment performance on every account during the previous 24 payment periods … Payments 120 days or more overdue would result in a default report being generated automatically.[34]

52.35 The CRAA's proposals intensified concern about its operations. In 1989, the New South Wales Privacy Committee concluded that the CRAA proposals represented a 'new and significant threat to privacy' and again recommended regulation of credit reporting.[35] In April 1989, CRAA announced that it would postpone the introduction of

---

30 New South Wales Government Privacy Committee, *Annual Report 1984* (1984), 30.

31 Ibid, 31.

32 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 2.

33 As discussed in Ch 55, the ALRC is of the view that such systems are better described as 'comprehensive' or 'more comprehensive' credit reporting.

34 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 6.

35 New South Wales Government Privacy Committee, *Annual Report* (1989), 23.

the PPS until January 1990, at the request of the Commonwealth Minister for Consumer Affairs, the Hon Senator Nick Bolkus.

52.36 On 19 April 1989, a 'Summit' was sponsored by the Australian Privacy Foundation. The meeting was attended by federal parliamentarians, CRAA representatives, state government agencies, credit providers, consumer and civil liberties groups and the Australian Computer Society.[36] At the conclusion of the Summit, the Minister for Consumer Affairs announced that the Australian Government intended to extend the *Privacy Act* to cover consumer credit reporting. Credit reporting would therefore become subject to national legislation for the first time.

Legislative history

52.37 As enacted, the *Privacy Act* had limited application to the private sector. The Act set out the Information Privacy Principles (IPPs), which regulated the collection, handling and use of personal information by Commonwealth public sector agencies.[37] The Act also provided guidelines for the collection, handling and use of individual tax file number information in both the public and private sectors following enhancements in the use of this unique identifier in 1988.[38]

Privacy Amendment Bill 1989

52.38 The Privacy Amendment Bill 1989 (Cth) was introduced on behalf of the Minister for Consumer Affairs on 16 June 1989. The Second Reading Speech stated that:

> The Privacy Amendment Bill 1989 is the next step in the Government's program to introduce comprehensive privacy protection for the Australian community. The principal purpose of this Bill is to provide privacy protection for individuals in relation to their consumer credit records.[39]

52.39 The Bill was intended to regulate the collection, use and disclosure of personal credit information by credit providers and credit reporting agencies. A central concern was that it was considered that there were 'inadequate controls on consumer credit reporting agencies to prevent them from using their databases for non consumer credit purposes'.[40]

---

36 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 6.

37 Since 1994, the IPPs also cover ACT public sector agencies: *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).

38 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).

39 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

40 Ibid.

52.40 The provisions would be supported by a code of conduct applying to information held in, or disseminated from, a central database and to the transfer of information between industry participants.[41] The Bill also provided individuals with an enforceable right of access to, and correction of, their credit records.

52.41 Significantly, the Bill restricted the categories of information that credit reporting agencies were permitted to include in individuals' credit information files. Essentially, credit reporting agencies were limited to collecting the kinds of information that they already held—that is, 'negative' information.[42]

52.42 The Second Reading Speech highlighted public concern about the privacy implications of a more comprehensive form of credit reporting. It was said that 'the credit reporting agency would effectively become a central clearing house of information about the current financial commitments of all Australians'.

> Positive reporting would constitute a major change in the level of information collected on individuals. While the notion of information collected in a centralised agency is not new, the collection of personal information on individuals' spending habits is—credit and spending profiles of individuals would have been built up through all their credit transactions.[43]

52.43 The Australian Government did not consider that there was 'any proven substantial benefit from positive reporting proposals'. In view of such strong privacy concerns, it concluded that any such expansion was 'impossible to condone'.[44]

Senate deliberations

52.44 The Privacy Amendment Bill 1989 was the subject of intense debate in the Senate. During the passage of the Bill, some 120 amendments from the Government, the Opposition and the Australian Democrats were proposed.[45]

52.45 On 2 November 1989, the Minister for Consumer Affairs tabled amendments to the Bill as introduced. These amendments were the result of consultations with the credit reporting industry and consumer and privacy groups and were said to clarify aspects of the regulatory scheme.[46]

---

41 Ibid.
42 The permitted content of credit information files is discussed in Chs 51–52.
43 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).
44 Ibid.
45 Commonwealth, *Parliamentary Debates*, Senate, 12 November 1990, 3939 (M Tate—Minister for Justice and Consumer Affairs).
46 Commonwealth, *Parliamentary Debates*, Senate, 2 November 1989, 2788 (N Bolkus—Minister for Consumer Affairs).

52.46 Specifically, the amendments were intended to:

- widen the classes of businesses that would be able to access a credit reporting agency;
- enable credit information to be used to assist credit providers in combating serious credit infringements and in collecting debts; and
- allow commercial and consumer credit reports to be cross-referenced by credit providers when making lending decisions.[47]

52.47 Following the return of the Hawke Government in March 1990, the Privacy Amendment Bill 1989 was restored to the Senate Notice Paper on 31 May. On 23 August 1990, the Bill was referred to the Senate Standing Committee on Legal and Constitutional Affairs (the Senate Standing Committee) for inquiry and report.

52.48 The Senate Standing Committee report, recommending 64 amendments to the Bill, was presented to the Senate on 22 October 1990.[48] In debate on 12 November, the Government moved 23 modifications to the amendments as recommended in the report.[49]

52.49 The Bill received a third reading, before passing with the support of the Democrats and the independent Senator Brian Harradine. The Bill was returned from the House of Representatives without amendment on 6 December 1990.

Privacy Amendment Act 1990

52.50 The *Privacy Amendment Act 1990* (Cth) received Royal Assent on 24 December 1990. The Privacy Amendment Bill 1989 had been described by the CRAA as containing 'the most restrictive credit reference laws in the Western world'. Professor Graham Greenleaf observed that:

> The credit industry launched a concerted campaign against the Bill, and obtained numerous amendments, but the 1989 Bill remained substantially intact when enacted.[50]

52.51 Heralding the enactment of the legislation, Greenleaf noted that the credit reporting industry, in attempting to expand its activities into more comprehensive reporting, had 'provoked a degree of legislative control which it had avoided in the

---

47 Ibid. See also, Supplementary Explanatory Memorandum, Privacy Amendment Bill 1989 (Cth).

48 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *The Privacy Amendment Bill 1989 [1990]* (1990).

49 Commonwealth, *Parliamentary Debates*, Senate, 12 November 1990, 3927 (B Cooney).

50 G Greenleaf, 'The Most Restrictive Credit Reference Laws in the Western World?' (1992) 66 *Australian Law Journal* 672, 672.

past'.[51] The legislation not only limited further expansion of credit reporting but was seen as 'rolling back the clock' by restricting certain existing practices, such as the provision of credit reports to real estate agents to check prospective tenants and mercantile agents to search for debtors' addresses.[52]

> It is rare for privacy legislation in any country to attempt such a retrospective repeal of the extension of data surveillance … This is the major achievement of the legislation: as a matter of public policy, it rejects the development of a multi-purpose reporting system as an unacceptable invasion of privacy—at least in the private sector.[53]

52.52 In order to allow the credit reporting industry time to comply with the new regulatory scheme, and to permit the Privacy Commissioner to issue a credit reporting code of conduct,[54] the Act did not commence operation until 24 September 1991. Before that date, transitional provisions were enacted,[55] deferring the commencement of the credit reporting provisions and the obligation to comply with the *Credit Reporting Code of Conduct* until 25 February 1992.[56]

Credit Reporting Code of Conduct

52.53 On 11 September 1991, the Privacy Commissioner issued the *Credit Reporting Code of Conduct* under s 18A of the *Privacy Act*. As required by the Act, the Privacy Commissioner consulted with government, commercial, consumer and other relevant bodies and organisations during the development of the Code. The Code became fully operational in February 1992 and was amended in 1995. Since then, amendments to the *Credit Reporting Code of Conduct* and explanatory notes have been made periodically, including to take into account changes made to the credit reporting provisions of the *Privacy Act*.[57]

Subsequent amendments

52.54 Amendments were made to the credit reporting provisions even before the *Privacy Amendment Act 1990* commenced operation. The *Law and Justice Legislation Amendment Act 1991* (Cth)[58] made amendments, among other things, to:

- clarify the definition of 'credit reporting business';
- provide that agents of credit providers can be treated as credit providers;

---

51 Ibid, 672.
52 Ibid, 674.
53 Ibid, 674.
54 As required by *Privacy Act 1988* (Cth) s 18A(1).
55 *Law and Justice Legislation Amendment Act 1991* (Cth) s 21.
56 Unless an act or practice breached *Privacy Act 1988* (Cth) ss 18H–18J concerning individuals' access to credit information files and credit reports, and the obligations of credit reporting agencies and credit providers to alter files and reports to ensure accuracy.
57 See Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), 2.
58 *Law and Justice Legislation Amendment Act 1991* (Cth) pt 3, ss 10–20.

- permit individuals to authorise other persons to have access to their credit information file or credit report;

- ensure that credit providers can consider telephone applications for credit;

- permit information to be used for internal management purposes by credit providers;

- provide for notices in the case of joint applications for credit; and

- permit disclosure of personal information by credit providers to guarantors, mortgage insurers, dispute resolution bodies, in credit card and EFTPOS transactions and mortgage securitisation.

52.55 Since the commencement of the *Privacy Amendment Act 1990*, there have been a series of amendments to the credit reporting provisions. The first set of amendments was contained in the *Law and Justice Legislation Amendment Act (No 4) 1992* (Cth) and related to securitisation, then a relatively new development in the financial sector. Securitisation refers to a complex method of financing loans under which, for example, a mortgage financed ostensibly by a credit provider, such as a credit union or building society, ultimately may be financed under mortgage securitisation using funds invested by investors in a trust.[59] Although the credit reporting provisions of the *Privacy Act* already made some provision for securitisation, it was necessary to substitute these provisions with more comprehensive ones given the complexity of the industry.[60]

52.56 The *Law and Justice Legislation Amendment Act 1993* (Cth) amended provisions governing disclosure of credit information by credit providers to state and territory authorities that administer mortgage assistance schemes to facilitate the giving of mortgage credit to individuals.

52.57 The *Law and Justice Legislation Amendment Act 1997* (Cth) amended the credit reporting provisions to:

- insert a definition of the term 'guarantee';

- give the Privacy Commissioner the power to determine that a federal agency is a credit provider; and

- allow an overdue payment under a guarantee to be listed on the guarantor's credit information file.

---

59 Explanatory Memorandum, Law and Justice Legislation Amendment Bill (No 4) 1992 (Cth).
60 Ibid.

52.58 The *Financial Sector Reform (Amendments and Transitional Provisions) Act (No 1) 1999* (Cth) changed the definition of credit provider in s 11B by repealing s 11B(1)(b)(i) and (ii), which referred to building societies and credit unions respectively.

52.59 The *Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001* (Cth) amended various offence provisions under Part IIIA to require an intention to breach certain provisions of Part IIIA, as distinct from reckless or misleading behaviour.

52.60 Finally, amendments providing for non-disclosure of reports made to certain law enforcement agencies under s 18K(5) were made by the *National Crime Authority Legislation Amendment Act 2001* (Cth), *Australian Crime Commission Establishment 2002* (Cth) and *Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006* (Cth).

53. Credit Reporting Provisions

Contents

Introduction

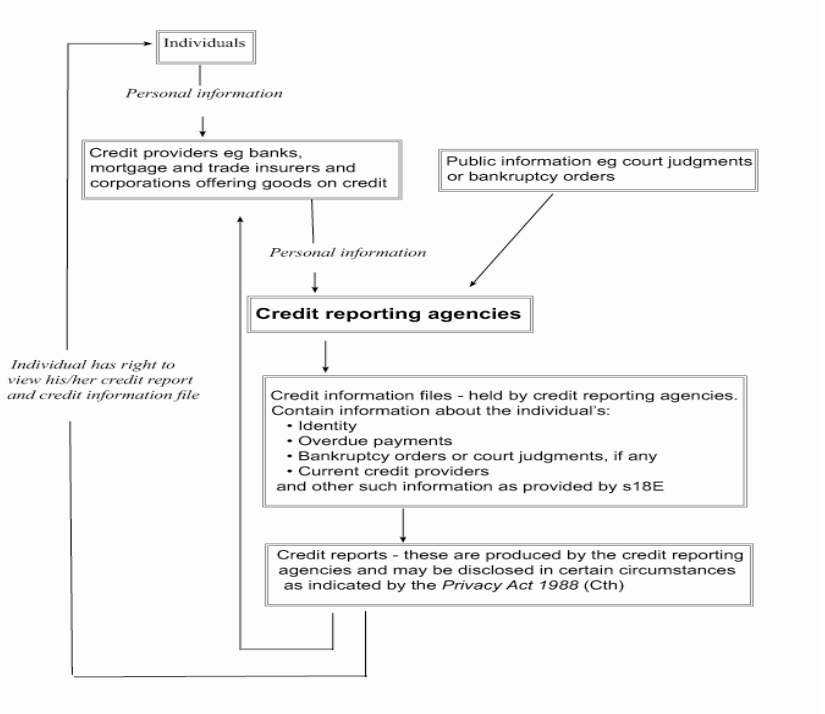
53.1 This chapter provides an overview of the credit reporting provisions of the *Privacy Act 1988* (Cth). Part IIIA of the *Privacy Act* contains the substantive provisions that regulate credit reporting. Some provisions dealing with the scope and application of the credit reporting provisions are located elsewhere in the Act. In addition, the Act empowers the Privacy Commissioner to issue a binding Code of

Conduct.[1] A *Credit Reporting Code of Conduct* came into effect on 24 September 1991.

53.2 The chapter first considers the people and information covered by the credit reporting provisions. How personal information may be used and disclosed in the credit reporting process, and how the Act provides for rights of access and correction for individuals in relation to their personal information are summarised. The chapter then considers the relationship between Part IIIA of the Act and the National Privacy Principles (NPPs).[2]

53.3 The chapter also describes the responsibilities and powers of the Office of the Privacy Commissioner (OPC) with regard to credit reporting[3] and the remedies and penalties in the event of non-compliance with the credit reporting provisions.[4]

53.4 Finally, this chapter sets out in detail how the *Privacy Act* permits and restricts the transfer of personal information in credit reporting. The diagram below is a summary of the main data flows under the present regulation of credit reporting.



1 *Privacy Act 1988* (Cth) ss 18A, 18B.
2 The NPPs are located in Ibid sch 3.
3 The powers and responsibilities of the OPC generally are discussed in Part F.
4 The remedies and penalties available under the *Privacy Act* generally also are discussed in Part F.

Application of the credit reporting provisions

53.5 This part of the chapter answers the following questions. What information is covered by the credit reporting provisions? To whom do the provisions apply?

Information covered by the provisions

53.6 A number of terms define the scope of the regulatory framework for credit reporting in the *Privacy Act*. The most important of these are 'personal information', 'credit information file' and 'credit report'. What follows is a discussion of the respective meanings and interrelationship of these terms.

53.7 The Act, principally in Part IIIA,[5] regulates the use and disclosure of 'personal information' for credit reporting purposes. 'Personal information' is defined to mean

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[6]

53.8 An individual's personal information may be collated by a credit reporting business to create a 'credit information file'. In relation to an individual, this means

> any record that contains information relating to the individual and is kept by a credit reporting agency in the course of carrying on a credit reporting business (whether or not the record is a copy of the whole or part of, or was prepared using, a record kept by another credit reporting agency or any other person).[7]

53.9 The credit information file in turn may be used to create a 'credit report'. It is in this form that an individual's personal information may pass from the person collecting the information (the credit reporting agency) to the person wishing to use the information (the credit provider).[8] The term 'credit report' is defined as

> any record or information, whether in a written, oral or other form, that:
>
> (a) is being or has been prepared by a credit reporting agency; and
>
> (b) has any bearing on an individual's:
>
> (i) eligibility to be provided with credit; or
>
> (ii) history in relation to credit; or
>
> (iii) capacity to repay credit; and

---

5 Note that other parts of the Act also relate to credit reporting. For instance, Part V deals with investigations by the Privacy Commissioner into alleged breaches of, among other things, the credit reporting rules.

6 *Privacy Act 1988* (Cth) s 6(1). The definition of 'personal information' is discussed in detail in Ch 6.

7 Ibid s 6(1).

8 The meanings of 'credit reporting agency' and 'credit provider' are discussed below.

> (c) is used, has been used or has the capacity to be used for the purpose of serving as a factor in establishing an individual's eligibility for credit.[9]

53.10 Section 18N applies to a third category of personal information contained in 'reports', a term which covers a much broader spectrum of documents than is encompassed by the term 'credit report'. Section 18N(9) states that 'report' means:

> (a) a credit report; or
>
> (b) … any other record or information, whether in a written, oral or other form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity;
>
> but does not include a credit report or any other record or information in which the only personal information relating to individuals is publicly available information.

Persons within the ambit of the provisions

53.11 There are four main categories of person affected by Part IIIA of the *Privacy Act*. These are: individuals; credit reporting agencies; credit providers; and third parties who provide personal information to credit reporting agencies.

Individuals

53.12 An individual whose personal information forms the basis of a credit information file may be affected by a credit report—especially in terms of the individual's application for credit. The Act stipulates that an individual must be 'a natural person' and that the definition of 'credit' does not include 'commercial credit'.[10]

53.13 This means that a corporation, for instance, cannot claim the protection of the credit reporting provisions in its own right. Commercial credit information only is regulated by the Act indirectly—where, for example, it is used to assess an application for consumer credit.[11]

Credit reporting agencies

53.14 The collection of personal information, its collation in credit information files and the disclosure of this information to credit providers only may be performed by a 'credit reporting agency'.[12] Section 11A provides that this term has two elements: a credit reporting agency must be a corporation and it must carry on a credit reporting business.

---

9 *Privacy Act 1988* (Cth) s 6(1).
10 Ibid s 6(1).
11 Ibid s 18L(4).
12 Ibid s 18C.

53.15 The requirement that a credit reporting agency must be a corporation is subject to a qualification. If the entity in question is engaged in wholly intra-state trade or commerce, and it is not engaged in banking or insurance (other than state banking or state insurance), then it is not regulated by Part IIIA.[13]

53.16 Section 6(1) of the Act defines the second element of a credit reporting agency—namely, that the agency carry on a 'credit reporting business'—as being:

> a business or undertaking (other than a business or undertaking of a kind in respect of which regulations made for the purposes of subsection (5C) are in force) that involves the preparation or maintenance of records containing personal information relating to individuals (other than records in which the only personal information relating to individuals is publicly available information), for the purpose of, or for purposes that include as the dominant purpose the purpose of, providing to other persons (whether for profit or reward or otherwise) information on an individual's:
>
> (a) eligibility to be provided with credit; or
>
> (b) history in relation to credit; or
>
> (c) capacity to repay credit;
>
> whether or not the information is provided or intended to be provided for the purposes of assessing applications for credit.

53.17 This second element remains subject to some exemptions. Information concerning an individual's commercial transactions is excluded.[14] Also, the regulations may exempt certain businesses from being considered credit reporting businesses for the purposes of the Act.[15] To date, however, no such regulations have been made.

Credit providers

53.18 In general, credit reporting agencies only may disclose information in credit information files to 'credit providers'. Credit providers, in turn, may use credit reports only for certain purposes—notably, in assessing a person's application for credit.

53.19 There is a finite list of categories of entities considered credit providers for the purposes of Part IIIA. This list does not include, for instance, real estate agents, debt collectors, employers and general insurers, and therefore they are not permitted to obtain credit reports.[16] Under the Act, the following are considered 'credit providers':

---

13 See Ibid s 18C(2). This qualification is discussed in detail later in this chapter.
14 Ibid s 6(5A).
15 Ibid s 6(5C).
16 Office of the Privacy Commissioner, *Credit Reporting: Key Requirements of Part IIIA* <www.privacy.gov.au/act/credit/index.html> at 24 August 2007.

- a bank;[17]
- a corporation, or an entity that is neither a corporation nor a government agency, that provides loans or issues credit cards as a substantial part of its business, or is carrying on a retail business;[18]
- an entity that provides loans (including by issuing credit cards), provided the Privacy Commissioner has made a determination in respect of such a class of entity;[19]
- a government agency that provides loans and is determined by the Privacy Commissioner to be a credit provider for the purposes of the Act;[20]
- a person who carries on a business involved in securitisation or managing loans that are subject to securitisation;[21] and
- an agent of a credit provider while the agent is carrying on a task necessary for the processing of a loan application, or managing a loan or account with the credit provider.[22]

53.20 The regulations also can exempt a corporation that would otherwise be considered a credit provider from being so regarded for the purposes of the Act.[23] To date, no such regulations have been made.

Persons providing personal information to credit reporting agencies

53.21 Finally, the credit reporting provisions also apply to a person, X, who provides personal information about another person, Y, to a third person, Z, carrying on a credit reporting business. Subject to certain constitutional limitations discussed later in this chapter, s 18D states that X must not give personal information about Y to Z unless Z is a corporation. Personal information is taken to be 'given' for the purposes of s 18D if the person to whom the information is given (ie, Z) 'is likely to use the information in the course of carrying on a credit reporting business'.[24]

---

17 *Privacy Act 1988* (Cth) s 11B(1)(a). The term 'bank' is defined in s 6(1) to mean: (a) the Reserve Bank of Australia; or (b) a body corporate that is an authorised deposit-taking institution for the purposes of the *Banking Act 1959* (Cth); or (c) a person who carries on 'State banking' within the meaning of s 51(xiii) of the *Constitution*.

18 *Privacy Act 1988* (Cth) s 11B(1)(b), (c).

19 Ibid s 11B(1)(b)(v). These determinations are discussed further in Ch 54.

20 Ibid s 11B(1)(d). Indigenous Business Australia is the only entity deemed to be a credit provider under this provision: Privacy Commissioner, *Credit Provider Determination No 2006–5 (Indigenous Business Australia)*, 25 October 2006.

21 *Privacy Act 1988* (Cth) s 11B(4A), (4B).

22 Ibid s 11B(5). The Act makes clear that 'the management of a loan' in subsection (5) does not include action taken to recover overdue loan repayments: s 11B(7).

23 Ibid s 11B(2).

24 Ibid s 18D(5).

Content of credit information files

53.22 A credit information file may contain information that is 'reasonably necessary … to identify the individual'.[25] Under s 18E(3), the Privacy Commissioner may determine 'the kinds of information that are … reasonably necessary to be included in an individual's credit information file in order to identify the individual'. Any such determination is said to be a 'disallowable instrument', which means that it must be tabled in the Australian Parliament and is then subject to disallowance.[26] In 1991, the Privacy Commissioner determined that the following kinds of information are 'reasonably necessary' to identify the individual:

i. full name, including any known aliases; sex; and date of birth;

ii. a maximum of three addresses consisting of a current or last known address and two immediately previous addresses;

iii. name of current or last known employer; and

iv. driver's licence number.[27]

53.23 The Act does not state that information purporting to identify an individual must be verified in any particular way or be of any particular standard *before* it is included in a credit information file. This may be relevant to such issues as identity theft.

53.24 As well as information reasonably necessary to identify the individual, s 18E provides an exhaustive list of the other categories of personal information that may be included in a credit information file. Anything that constitutes personal information, but is not included in this list, may not be included in a credit information file. The Act allows a credit reporting agency to hold personal information in an individual's credit information file only for a finite period, the length of which depends on the nature of the information in question. After this period has elapsed, the agency must delete the relevant information within one month.[28]

---

25 Ibid s 18E(1)(a).

26 Ibid s 18E(4)–(6). Note that s 18E(6) of the *Privacy Act* refers to s 46A of the *Acts Interpretation Act 1901* (Cth). However, the latter provision has been repealed. Section 6(d)(i) of the *Legislative Instruments Act 2003* (Cth) provides that an instrument said to be a disallowable instrument for the purposes of s 46A of the *Acts Interpretation Act* should be considered a legislative instrument for the purposes of the *Legislative Instruments Act*.

27 Privacy Commissioner, *Determination under the Privacy Act 1988: 1991 No 2 (s 18E(3)): Concerning Identifying Particulars Permitted to be Included in a Credit Information File*, 11 September 1991.

28 *Privacy Act 1988* (Cth) s 18F(1).

53.25 In summary, information may be included in a credit information file if it is a record of:

- a credit provider having sought a credit report in connection with an application for consumer or commercial credit, provided the record also states the amount of credit sought;[29]
- a credit provider having sought a credit report for the purpose of assessing the risk in purchasing, or undertaking credit enhancement of, a loan by means of securitisation;[30]
- a mortgage or trade insurer having sought a credit report in connection with the provision of mortgage or trade insurance to a credit provider;[31]
- a credit provider having sought a credit report in connection with the individual having offered to act as guarantor for a loan;[32]
- a credit provider being a current credit provider in relation to the individual;[33]
- credit provided by a credit provider to an individual, where the individual is at least 60 days overdue in making a payment on that credit and the credit provider has taken steps to recover some or all of the credit outstanding;[34]
- a cheque for $100 or more that has been dishonoured twice;[35]
- a court judgment or bankruptcy order made against the individual;[36]
- a credit provider's opinion that the individual has committed a specific serious credit infringement;[37]

---

29 Ibid s 18E(1)(b)(i). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

30 Ibid s 18E(1)(b)(ia). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

31 Ibid s 18E(1)(b)(ii), (iii). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

32 Ibid s 18E(1)(b)(iv). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

33 Ibid s 18E(1)(b)(v). The information may be kept for a maximum of 14 days after the credit reporting agency is notified that the credit provider is no longer the individual's credit provider: s 18F(2)(b).

34 Ibid s 18E(1)(b)(vi). The information may be kept for a maximum of five years after the credit reporting agency was informed of the overdue payment concerned: s 18F(2)(c).

35 Ibid s 18E(1)(b)(vii). The information may be kept for a maximum of five years after the second dishonouring of the cheque: s 18F(2)(d).

36 Ibid s 18E(1)(b)(viii), (ix). A record of judgment may be kept for a maximum of five years after the judgment was made: s 18F(2)(e). A record of a bankruptcy order may be kept for a maximum of seven years after the order was made: s 18F(2)(f).

37 Ibid s 18E(1)(b)(x). The information may be kept for a maximum of seven years after the information was included in the credit information file: s 18F(2)(g).

- an overdue payment to a credit provider by a person acting as guarantor to a borrower, provided the following conditions are met: the credit provider is not prevented by law from bringing proceedings to recover the overdue amount; the credit provider has given the guarantor notice of the borrower's default; 60 days have elapsed since the notice was given; and the credit provider has taken steps to recover the overdue payment from the guarantor;[38] and

- a note or annotation to be made to the individual's existing credit information file, pursuant to ss 18J(2), 18F(4) or 18K(5).[39]

53.26 Certain types of personal information must never be included in an individual's credit information file. That is, information recording an individual's:

- political, social or religious beliefs or affiliations;

- criminal record;

- medical history or physical handicaps;

- race, ethnic origins or national origins;

- sexual preferences or practices; or

- lifestyle, character or reputation.[40]

53.27 If a credit report contains personal information that does not fall within the permitted categories, a credit provider who holds the report must not use this personal information, and must not use the report at all until the relevant information has been deleted.[41] A breach of this requirement constitutes a credit reporting infringement.[42] In this situation, an individual may complain to the Privacy Commissioner that the credit provider has committed an interference with the individual's privacy.[43] The Privacy

---

38 Ibid s 18E(1)(ba). The information may be kept for a maximum of five years after the credit reporting agency was informed of the overdue payment: s 18F(2A).

39 Ibid s 18E(1)(c), (d); see also s 18E(7). Note that s 18J(2) obliges a credit reporting agency to include a statement of the correction, deletion or addition sought by an individual to his or her credit information file, where the agency has not made the relevant change; s 18F(4) requires a credit reporting agency, when appropriately informed, to include a note saying that the individual is no longer overdue in making a payment; and s 18K(5) requires a credit reporting agency to include a note on a person's credit information file when it has disclosed personal information from the file.

40 Ibid s 18E(2).

41 Ibid s 18L(3).

42 A breach of a provision of Part IIIA is a 'credit reporting infringement': Ibid s 6(1).

43 See Ibid ss 13(d), 36(1).

Commissioner then may carry out an investigation and issue a determination in accordance with Part V of the Act.[44]

Accuracy and security of personal information

53.28 Credit reporting agencies and credit providers have obligations to ensure the accuracy and security of personal information in their possession or control. Credit reporting agencies and credit providers are required to take reasonable steps to ensure that:

- personal information in a file or report is 'accurate, up-to-date, complete and not misleading';
- the file or report is protected against 'misuse' including 'unauthorised access, use, modification or disclosure'; and
- if an agency or credit provider gives the file or report to a person in connection with the provision of a service to the agency or credit provider, it must 'prevent unauthorised use or disclosure of personal information contained in the file or report'.[45]

53.29 Credit reporting agencies and credit providers are prohibited from disclosing to anyone a false or misleading credit report. If an agency or provider intentionally contravenes this provision, it is liable for a fine of up to $75,000.[46]

Disclosure of personal information

53.30 The *Privacy Act* restricts how, and to whom, personal information in credit information files and credit reports may be disclosed. As explained below, the Act largely focuses on regulating the actions of credit reporting agencies, credit providers and others—setting rules on what these entities may do. Part IIIA, however, also prohibits any other person from obtaining access to a credit information file or credit report, where the Act does not authorise the person to do so, or where the person gains access by a false pretence.[47]

Credit reporting agencies

53.31 Section 18K of the Act contains four general rules on how personal information may be conveyed by credit reporting agencies to people who are permitted to view the

---

44 The Privacy Commissioner's complaint-handling processes are discussed in Ch 49.
45 *Privacy Act 1988* (Cth) s 18G.
46 Ibid s 18R.
47 Ibid ss 18S, 18T. The penalty in respect of each offence is a fine not exceeding $30,000.

information. If a credit reporting agency intentionally contravenes any of the relevant provisions, it is liable for a fine of up to $150,000.[48]

53.32 The general rules are as follows. First, a credit reporting agency is not permitted to make a credit information file directly available to another entity; instead the agency must convey that information in the form of a credit report. Secondly, a credit report only may be given to a credit provider.[49] Thirdly, personal information in a credit report only may be disclosed by a credit reporting agency for one of the purposes specified in the Act—these are summarised below. Fourthly, a credit reporting agency must not disclose personal information if the information does not fall within the permitted categories in s 18E, or if the agency is required to delete the information in question under s 18F.[50] These rules, however, are subject to certain exceptions, which are also set out below.

53.33 The purposes for which an individual's credit report may be given to a credit provider are set out exhaustively in the section. They relate to the state of mind and activities of the credit provider. The permitted purposes are to:

- assess the individual's application for credit;[51]
- assess the risk in purchasing, or undertaking credit enhancement of, a loan by means of securitisation;[52]
- assess an application for commercial credit, provided the individual agrees to the disclosure;[53]
- assess whether to accept the individual as a guarantor of a loan, provided the individual agrees in writing to the disclosure;[54]
- inform a current credit provider that the individual is at least 60 days overdue in making a payment to a second credit provider and this second credit provider has taken steps to recover some or all of the credit outstanding;[55]
- assist in collecting overdue payments from the individual;[56] and

---

48 Ibid s 18K(5).
49 The terms 'credit report' and 'credit provider' are discussed earlier in this chapter.
50 *Privacy Act 1988* (Cth) s 18K(2).
51 Ibid s 18K(1)(a).
52 Ibid s 18K(1)(ab), (ac).
53 Ibid s 18K(1)(b). The individual's agreement must usually be given in writing—see s 18K(1A).
54 Ibid s 18K(1)(c).
55 Ibid s 18K(1)(f). The relevant credit reporting agency is permitted to make such a disclosure only where it has received this information at least 30 days before the disclosure.
56 Ibid s 18K(1)(g).

- assist in collecting overdue payments in respect of commercial credit, provided the individual consents or the commercial credit was given prior to 24 September 1991.[57]

53.34 There are some situations in which a credit reporting agency may disclose an individual's credit report to a person who is not a credit provider, including disclosure to: another credit reporting agency;[58] or a mortgage or trade insurer, where the insurer is assessing matters connected with whether to provide mortgage or trade insurance to a credit provider in respect of the individual.[59]

53.35 The rule prohibiting the direct disclosure of personal information from an individual's credit information file is subject to a number of exceptions, namely where the:

- only personal information disclosed is publicly available;[60]
- disclosure is required or authorised by law;[61] or
- credit reporting agency is satisfied that a credit provider or law enforcement authority reasonably believes the individual has committed a serious credit infringement and the information is given to a credit provider or law enforcement authority.[62]

Credit providers

53.36 The rules dealing with how a credit provider may disclose personal information in its possession are set out in ss 18N and 18NA of the Act. The general rule is that a credit provider is prohibited from disclosing an individual's personal information (either from a credit report or other credit worthiness information held by the credit provider and that is not publicly available) unless a stated exception applies. If a credit provider intentionally contravenes this provision, it is liable for a fine of up to $150,000.[63]

53.37 There is a finite list of exceptions to the general rule. In summary, a credit provider is permitted to disclose an individual's personal information to:

- a credit reporting agency that is creating or modifying a credit information file;[64]

---

57 Ibid s 18K(1)(h).
58 Ibid s 18K(1)(j).
59 Ibid s 18K(1)(d), (e). In respect of trade insurance, the disclosure is permitted only if the individual has agreed in writing: s 18K(1)(e).
60 Ibid s 18K(1)(k).
61 Ibid s 18K(1)(m).
62 Ibid s 18K(1)(n).
63 Ibid s 18N(2).
64 Ibid s 18N(1)(a).

- another credit provider for a particular purpose, provided either the individual specifically agrees or it is in connection with an overdue payment;[65]
- the guarantor of an individual's loan in connection with enforcing the guarantee;[66]
- a mortgage insurer for the purpose of risk assessment or as required by the contract between the credit provider and the insurer;[67]
- a recognised dispute settling body that is assisting in settling a dispute between the credit provider and the individual;[68]
- a government body with responsibility in this area;[69]
- a supplier of goods or services for the purpose of determining whether to accept a payment by credit card or funds transfer, provided the personal information disclosed does no more than identify the individual and inform the supplier whether the individual has sufficient funds for the proposed payment;[70]
- a person considering taking on the individual's debt, provided the personal information disclosed does no more than identify the individual and inform the person of the amount of the debt;[71]
- the guarantor, or a proposed guarantor, of a loan, provided the borrower specifically agrees;[72]
- a debt collector in respect of overdue payments to the credit provider, provided the personal information disclosed does no more than: identify the individual; give specified details relating to the debt; and provide a record of any adverse court judgments or bankruptcy orders;[73]

---

65 Ibid s 18N(1)(b), (fa).
66 Ibid s 18N(1)(ba).
67 Ibid s 18N(1)(bb).
68 Ibid s 18N(1)(bc).
69 Ibid s 18N(1)(bd), (bda).
70 Ibid s 18N(1)(be).
71 Ibid s 18N(1)(bf).
72 Ibid s 18N(1)(bg), (bh). The borrower's agreement is not necessary if: the guarantee (or security) was provided before 7 December 1992; the information discloses the guarantor's liability; and the credit provider previously advised the borrower that such disclosures may take place: s 18N(1)(bg)(ii). See also s 18NA in respect of indemnities.
73 Ibid s 18N(1)(c). If the debt relates to commercial credit, the credit provider is prohibited from disclosing the details of the debt to a debt collector: s 18N(1)(ca).

- a corporation related to the credit provider that is itself a corporation;[74]
- a corporation, in connection with its taking on a debt owed to the credit provider;[75]
- a person who manages loans made by the credit provider;[76]
- a person, as required or authorised by law;[77]
- the individual or another person authorised by the individual;[78] and
- another credit provider or a law enforcement authority, where the credit provider reasonably suspects the individual has committed a serious credit infringement.[79]

53.38 The Privacy Commissioner has a power to determine the manner in which such a report may be disclosed;[80] however, the Commissioner is yet to make such a determination.

Information given by credit providers to credit reporting agencies

53.39 In practice, credit reporting agencies, in compiling credit information files, obtain most of that information from credit providers themselves.[81] This creates a two-way flow of personal information between credit reporting agencies and credit providers.

53.40 In view of this, the Act limits the information that a credit provider may provide to a credit reporting agency. That is, a credit provider must not give to a credit reporting agency personal information relating to an individual in any of the following situations:

- where the information would not fall within the categories in s 18E(1) summarised above;
- where the credit provider does not have reasonable grounds for believing the information is correct; or

74 Ibid s 18N(1)(d).
75 Ibid s 18N(1)(e).
76 Ibid s 18N(1)(f).
77 Ibid s 18N(1)(g).
78 Ibid s 18N(1)(ga), (gb).
79 Ibid s 18N(1)(h).
80 Ibid s 18N(5)–(7).
81 This is specifically anticipated in Ibid ss 18E(8) and 18N(1)(a).

- where the credit provider did not, before or at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a credit reporting agency.[82]

Use of personal information

Credit providers

53.41 Section 18L(1) of the Act states the general rule that a credit provider may only use an individual's credit report, or personal information it derives from the credit report, for the purpose of assessing the individual's application for credit, or for one of the other permitted purposes for which the report was originally given to the credit provider.[83] If a credit provider intentionally contravenes this provision, it is liable for a fine of up to $150,000.[84]

53.42 The rule in s 18L(1) is subject to the following exceptions, which allow a credit provider to use a credit report:

- as required or authorised by law;[85]

- if the credit provider reasonably believes the individual has committed a serious credit infringement, and the information is used in connection with the infringement;[86] or

- in connection with an individual's commercial activities or commercial credit worthiness, provided the individual agrees.[87]

Use and disclosure by mortgage and trade insurers

53.43 Mortgage and trade insurers must only use personal information contained in an individual's credit report only in connection with assessing the risk in providing such insurance to the individual's credit provider, or as required or authorised by law.[88] They must not disclose personal information from a credit report to any person unless required or authorised by law.[89] If a mortgage or trade insurer 'knowingly or

---

82 Ibid s 18E(8).
83 The other permitted purposes are summarised earlier in this chapter.
84 *Privacy Act 1988* (Cth) s 18L(2).
85 Ibid s 18L(1)(e).
86 Ibid s 18L(1)(f).
87 Ibid s 18L(4), (4A). The Privacy Commissioner has a power to determine how this information may be used and how an individual's consent may be obtained: s 18L(6)–(8). To date, this power has not been exercised.
88 Ibid s 18P(1), (2). Mortgage insurers also may use such information pursuant to the contract between the mortgage insurer and the credit provider: s 18P(1)(c).
89 Ibid s 18P(5).

recklessly' contravenes any of these provisions, it is liable for a fine of up to $150,000.[90]

Use and disclosure by other persons

53.44 There are specific rules on how other persons may use personal information that they have obtained from a credit provider or credit reporting agency. Any person who intentionally contravenes one of these provisions will be liable for a fine of up to $30,000.[91] The rules are as follows:

- Where a credit provider discloses information to a related corporation, the related corporation is subject to the use and disclosure limitations that apply to the credit provider. The same rules also apply where a credit report is received by a person who was deemed to be a credit provider because it was engaged in securitisation of a loan, but has since ceased to be a credit provider.[92]

- Where information is received by a corporation, in connection with its taking on a debt owed to the credit provider, the corporation may use the information only in considering whether to take on the debt. If it takes on the debt, the corporation may use the information in connection with exercising its rights. Similar rules apply to a professional legal adviser or financial adviser in connection with advising the corporation about these matters, or as required or authorised by law.[93]

- Where information is received by a person who manages loans made by the credit provider, the information only may be used for managing these loans, or as required or authorised by law.[94]

Consent and credit reporting

53.45 While Part IIIA generally does not require the agreement of individuals to the use or disclosure of credit reporting information about them, provided notification has been given, consent is required in some contexts, which are discussed below.

Consent to disclosure of information

53.46 Part IIIA contains provisions that require the agreement of an individual to the disclosure of his or her personal information. Under s 18K, an individual's agreement, sometimes in writing, is required in relation to the disclosure by a credit reporting agency of information contained in a credit report to a:

---

90 Ibid s 18P(6).
91 Ibid s 18Q(9).
92 Ibid s 18Q(1), (6)–(7A).
93 Ibid s 18Q(2), (3). See also s 18Q(8).
94 Ibid s 18Q(4). See also s 18Q(8).

- credit provider for the purpose of assessing an application for commercial credit;[95]

- credit provider for the purpose of assessing whether to accept an individual as a guarantor;[96]

- trade insurer for the purpose of assessing insurance risks in relation to commercial credit;[97] and

- credit provider for the purpose of collecting payments overdue in respect of commercial credit.[98]

53.47 Section 18L(4) requires an individual specifically to have agreed to a credit provider using information concerning commercial credit in assessing an application for consumer credit. Finally, under s 18N, an individual must have 'specifically agreed' to the disclosure of a credit report or other credit worthiness information by a credit provider to another credit provider for the particular purpose;[99] to a guarantor for a loan given by the credit provider to the individual concerned;[100] and to a person considering whether to offer to act as a guarantor.[101]

Disclosure to a credit reporting agency

53.48 Part IIIA does not require an individual to consent to disclosure of information by a credit provider to a credit reporting agency.[102] An individual's consent may be required, however, by the NPPs or by common law duties of confidence owed by some credit providers to their customers.

53.49 Consent to disclosure may be required—at least where the credit provider is a bank[103]—to avoid breaching the duty of confidence owed by banks to their customers. This common law duty was defined in *Tournier v National Provincial and Union Bank of England*.[104] It is reflected in the Australian Bankers' Association's *Code of Banking*

---

95 Ibid s 18K(1)(b).
96 Ibid s 18K(1)(c).
97 Ibid s 18K(1)(e).
98 Ibid s 18K(1)(h).
99 Ibid s 18N(1)(b).
100 Ibid s 18N(1)(bg).
101 Ibid s 18N(1)(bh).
102 A credit provider, however, must not give personal information to a credit reporting agency unless the individual concerned has been informed that the information might be disclosed to a credit reporting agency: Ibid s 18E(8).
103 The duty also may apply to building societies, credit unions and other authorised deposit-taking institutions: A Tyree, 'Does Tournier Apply to Building Societies?' (1995) 6 *Journal of Banking and Finance Law and Practice* 206.
104 *Tournier v National Provincial & Union Bank of England* [1924] 1 KB 461. The duty extends to disclosure to related bodies corporate: *Bank of Tokyo Ltd v Karoon* [1987] AC 45, 53–54.

Practice, which provides that, in addition to a bank's duties under legislation, it has a general duty of confidentiality towards a customer except in the following circumstances: where disclosure is compelled by law; where there is a duty to the public to disclose; where the interests of the bank require disclosure; or where disclosure is made with the express or implied consent of the customer.[105]

53.50 Chapter 19 discusses the role of consent in privacy regulation generally. As noted in Chapter 19, problems arise where an individual's capacity to give true consent is hampered. This issue is seen most commonly in the context of 'bundled consent'—the practice of bundling together consent to a wide range of uses and disclosures of personal information without giving individuals the option of selecting to which uses and disclosures they agree.[106]

Rights of access, correction and notification

53.51 Credit reporting agencies and credit providers in possession or control of an individual's credit information file or credit report must take reasonable steps to allow the individual access to the file or report. The individual can authorise another person (who is not a credit provider or a trade or mortgage insurer) to exercise these same rights in connection with applying for a loan, or advice in relation to a loan.[107]

53.52 Credit reporting agencies and credit providers must, in relation to credit information files and credit reports in their possession or control, 'take reasonable steps, by way of making appropriate corrections, deletions and additions, to ensure that personal information in the file or report is accurate, up-to-date, complete and not misleading'. If so requested, the agency or provider must either amend personal information in a file or report as requested by the individual concerned, or include a statement of the correction, deletion or addition sought by the individual.[108]

53.53 Credit providers also have notification obligations when they use a credit report to refuse an application for credit. Where a credit provider refuses an application for credit, and this refusal relates partly or wholly to information in an individual's credit report, the credit provider must: notify the individual of these facts and of the individual's right to access his or her credit report; and provide the name and address of the relevant credit reporting agency.[109]

53.54 Where a joint application for credit is refused, and this refusal relates partly or wholly to information in the credit report of one of the applicants or proposed guarantors, the credit provider must inform the other applicants that the application

---

105 Australian Bankers' Association, *Code of Banking Practice* (1993), [12.1].

106 See also Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [53.99]–[53.117].

107 *Privacy Act 1988* (Cth) s 18H.

108 Ibid s 18J.

109 Ibid s 18M(1).

was refused for this reason.[110] In this situation, however, the credit provider does not have to provide any further information, as the other applicants do not have a right to view the credit report of this person.

Responsibilities and powers of the OPC

53.55 The *Privacy Act* gives the OPC a range of responsibilities and powers under the Act.[111] These responsibilities and powers were described in more detail in Part F of this Report. This chapter describes aspects of the OPC's responsibilities and powers in relation to:

- issuing a code of conduct relating to credit information files and credit reports;[112]
- making certain determinations, on the Privacy Commissioner's initiative, under the credit reporting provisions of the *Privacy Act*;[113]
- auditing credit information files and credit reports held by credit reporting agencies and credit providers;[114] and
- investigating credit reporting infringements,[115] either in response to a complaint or on the OPC's initiative,[116] and making determinations after investigating complaints.[117]

Credit Reporting Code of Conduct

53.56 Under s 18A of the *Privacy Act*, the Privacy Commissioner must, after consulting government, commercial, consumer and other relevant bodies,[118] issue a code of conduct concerning:

> (a) the collection of personal information for inclusion in individuals' credit information files; and
>
> (b) the storage of, security of, access to, correction of, use of and disclosure of personal information included in individuals' credit information files or in credit reports; and

---

110 Ibid s 18M(2), (3).
111 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Ch 6.
112 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) issued under the *Privacy Act 1988* (Cth) s 18A.
113 *Privacy Act 1988* (Cth) ss 11B(1), 18E(3), 18K(3), 18L(6), 18N(5).
114 Ibid s 24A(1)(g).
115 A 'credit reporting infringement' is defined as a breach of either the *Credit Reporting Code of Conduct* or the provisions of pt IIIA: Ibid s 6.
116 Ibid pt V.
117 Ibid s 52.
118 Ibid s 18A(2).

> (c) the manner in which credit reporting agencies and credit providers are to handle disputes relating to credit reporting; and
>
> (d) any other activities, engaged in by credit reporting agencies or credit providers, that are connected with credit reporting.[119]

53.57 In preparing the code of conduct, the Commissioner must have regard to the Information Privacy Principles (IPPs), the NPPs, Part IIIA of the Act and the likely costs to credit reporting agencies and credit providers of complying with the code.[120]

53.58 The *Credit Reporting Code of Conduct* (Code of Conduct) came into effect on 24 September 1991 and remains in force. The Code of Conduct is legally binding. Section 18B of the *Privacy Act* provides that a credit reporting agency or credit provider must not do an act, or engage in a practice, that breaches the Code of Conduct. Breach of the Code of Conduct constitutes a credit reporting infringement and an interference with privacy under s 13 of the Act.[121]

53.59 In broad terms, the Code of Conduct supplements Part IIIA on matters of detail not addressed by the Act. Among other things, the Code of Conduct requires credit providers and credit reporting agencies to:

- deal promptly with individual requests for access to, and amendment of, personal credit information;
- ensure that only permitted and accurate information is included in an individual's credit information file;
- keep adequate records in regard to any disclosure of personal credit information;
- adopt specific procedures in settling credit reporting disputes; and
- provide staff training on the requirements of the *Privacy Act*.[122]

53.60 The Code of Conduct is accompanied by Explanatory Notes, which explain how Part IIIA and the Code interact. For example, in relation to the permitted content of credit information files, the Code of Conduct provides that:

> A credit reporting agency recording an enquiry made by a credit provider in connection with an application for credit may include, within the record of the enquiry, a general indication of the nature of the credit being sought.[123]

---

119 Ibid s 18A(1). The Code of Conduct is a disallowable instrument: *Privacy Act 1988* (Cth) s 18A(4).
120 *Privacy Act 1988* (Cth) s 18A(3).
121 Ibid s 13(d).
122 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), 3.
123 Ibid, [1.1].

53.61 The Explanatory Notes explain that, while s 18E(1) expressly permits inclusion of a record of an enquiry made by a credit provider in connection with an application for credit, together with the amount of credit sought:

> because of the size of the credit reporting system, and the large number and variety of credit applications recorded every year, it is accepted that an account type indicator should be allowed to be included in the file in order to facilitate speedy and accurate identification verification by credit providers of the enquiries recorded in credit information files.[124]

Determinations

53.62 The Privacy Commissioner has power to make certain determinations under the credit reporting provisions of the *Privacy Act*, including[125] determinations relating to:

- the definition of 'credit provider';[126] and
- the kinds of identifying information reasonably necessary to be included in credit information files.[127]

Credit provider determinations

53.63 Under Part IIIA, access to personal information provided by credit reporting agencies generally is restricted to businesses that are credit providers. Section 11B defines 'credit providers' for the purposes of the Act. In summary, under s 11B, financial organisations such as banks, building societies, credit unions and retail businesses that issue credit cards are automatically classed as credit providers.

53.64 Other businesses also are credit providers if they provide loans—defined to include arrangements under which a person receives goods or services with payment deferred, such as under a hire-purchase agreement[128]—and are included in a class of corporations determined by the Privacy Commissioner to be credit providers for the purpose of the Act.[129]

53.65 The Privacy Commissioner has made three determinations under s 11B of the Act. These include a determination that corporations are to be regarded as credit providers if they:

---

124 Ibid, Explanatory Notes, [1]–[2].

125 Other determinations by the Privacy Commissioner have been issued under *Privacy Act 1988* (Cth) s 18K(3)(b)—permitting the disclosure of certain information included in a credit information file or other record before the commencement of s 18K (24 September 1991).

126 Ibid s 11B(1).

127 Ibid s 18E(3).

128 Ibid s 6.

129 Ibid s 11B(1)(v)(B).

- make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least seven days; or

- engage in the hiring, leasing or renting of goods, where no amount, or an amount less than the value of the goods, is paid as deposit for return of the goods, and the relevant arrangement is one of at least seven days duration.[130]

53.66 Another determination deems corporations to be credit providers where they have acquired the rights of a credit provider with respect to the repayment of a loan (whether by assignment, subrogation or other means).[131]

53.67 Both these determinations are discussed further in Chapter 54, in relation to the definition of credit provider for the purposes of the new *Privacy (Credit Reporting Information) Regulations*.[132]

Identifying information

53.68 The Privacy Commissioner may determine the kinds of information that are, for the purposes of s 18E(1)(a), 'reasonably necessary to be included in an individual's credit information file in order to identify the individual'.[133] The Privacy Commissioner made a determination under this provision in 1991.[134]

Audits of credit information files

53.69 The Privacy Commissioner has power to audit credit information files and credit reports held by credit reporting agencies and credit providers.[135] The purpose of such audits is to ascertain whether credit information files and credit reports are being maintained in accordance with the Code of Conduct and Part IIIA of the *Privacy Act*.

53.70 The Privacy Commissioner also may examine the records of credit reporting agencies and credit providers to ensure that they are not using personal information in those records for unauthorised purposes, and are taking adequate steps to prevent unauthorised disclosure of those records.[136]

---

130 Privacy Commissioner, *Credit Provider Determination No. 2006–4 (Classes of Credit Providers)*, 21 August 2006.

131 Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006.

132 The third determination involves a specific corporation: Privacy Commissioner, *Credit Provider Determination No 2006–5 (Indigenous Business Australia)*, 25 October 2006.

133 *Privacy Act 1988* (Cth) s 18E(3).

134 Privacy Commissioner, *Determination under the Privacy Act 1988: 1991 No 2 (s 18E(3)): Concerning Identifying Particulars Permitted to be Included in a Credit Information File*, 11 September 1991.

135 *Privacy Act 1988* (Cth) s 28A(1)(g).

136 Office of the Privacy Commissioner, *Credit Information Audit Process* <www.privacy.gov.au/publications> at 5 May 2008, 1.

Investigating credit reporting infringements

53.71 Part V, Division 1 of the *Privacy Act* deals with the investigation of complaints and investigations on the Privacy Commissioner's initiative.[137] These provisions must be considered in association with the dispute settling procedures relating to credit reporting, which are set out in the Code of Conduct.

53.72 Under s 36(1) of the *Privacy Act*, an individual may complain to the Privacy Commissioner about 'an act or practice that may be an interference with the privacy of the individual'. In the case of an act or practice engaged in by a credit reporting agency or credit provider, an act or practice is an interference with the privacy of an individual if it 'constitutes a credit reporting infringement in relation to personal information that relates to the individual'.[138] In turn, a 'credit reporting infringement' means a breach of the Code of Conduct or a breach of a provision of Part IIIA of the Act.[139] Subject to certain exceptions, the Privacy Commissioner must investigate an act or practice that may be an interference with the privacy of an individual if a complaint has been made under s 36.[140]

53.73 Under Part V, Division 2 of the *Privacy Act*, the Privacy Commissioner may make a determination after investigating a complaint. Under s 52, if the complaint is found to be substantiated, the determination may include declarations that the respondent not repeat or continue the conduct; or provide redress or compensation for any loss or damage suffered by the complainant.[141] The Privacy Commissioner also may order that a respondent make an appropriate correction, deletion or addition to a record, or attach to a record a statement provided by the complainant.[142]

53.74 Under s 41(2), the Privacy Commissioner may decide not to investigate, or to defer investigation, if satisfied that the respondent has dealt, or is dealing, adequately with the complaint; or if the respondent has not yet had an adequate opportunity to deal with the complaint.

53.75 The Code of Conduct sets out dispute-settling procedures that must be followed by credit reporting agencies and credit providers.[143] The Code provides, among other things, that:

---

137 These provisions are discussed in more detail in Ch 49.
138 *Privacy Act 1988* (Cth) s 13(d).
139 Ibid s 6(1).
140 Ibid s 40(1).
141 Ibid s 52(1)(b).
142 Ibid s 52(3B).
143 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), pt 3.

- credit reporting agencies and credit providers must handle credit reporting disputes in a fair, efficient and timely manner;[144]

- where a credit reporting agency establishes that it is unable to resolve a dispute, it must inform the individual concerned immediately that it is unable to resolve the dispute and that the individual may complain to the Privacy Commissioner;[145] and

- a credit provider should refer a dispute between that credit provider and an individual to a credit reporting agency for resolution where the dispute concerns the contents of a credit report issued by the credit reporting agency.[146]

Remedies and penalties

53.76 Part IIIA creates a range of credit reporting offences, including offences in relation to:

- non-corporations carrying on a credit reporting business;[147]

- persons giving personal information to a non-corporation carrying on a credit reporting business;[148]

- credit reporting agencies disclosing personal information other than as permitted;[149]

- credit providers using personal information contained in credit reports other than as permitted;[150]

- credit providers disclosing credit worthiness information other than as permitted;[151]

- credit reporting agencies or credit providers intentionally giving out a credit report that contains false or misleading information;[152]

---

144 Ibid, [3.1].
145 Ibid, [3.2].
146 Ibid, [3.3].
147 *Privacy Act 1988* (Cth) s 18C(4).
148 Ibid s 18D(4).
149 Ibid s 18K(4).
150 Ibid s 18L(2).
151 Ibid s 18N(2).
152 Ibid s 18R(2).

- persons intentionally obtaining unauthorised access to credit information files or credit reports;[153] and

- persons obtaining access to credit information files or credit reports by false pretences.[154]

53.77 The mechanisms available to ensure enforcement of the *Privacy Act* generally, including remedies following the OPC's own motion investigations, determinations, reports, injunctions and penalties, are discussed in detail in Chapter 50.

153 Ibid s 18S(3).
154 Ibid s 18T.

54. Approach to Reform

Contents

Introduction

54.1 This chapter introduces the ALRC's recommendations for reform of the credit reporting provisions of the *Privacy Act 1988* (Cth). The starting point for these recommendations is that Part IIIA and its related provisions should be repealed and credit reporting regulated under the general provisions of the *Privacy Act* and the model Unified Privacy Principles (UPPs).[1] Under this regime, privacy regulation specific to credit reporting would be set out in regulations promulgated under the Act—referred to for the purposes of this Report as the *Privacy (Credit Reporting Information) Regulations.*

54.2 The reasons for recommending the repeal of the credit reporting provisions and the promulgation of the *Privacy (Credit Reporting Information) Regulations* include the:

- desirability of amending the Act to achieve greater logical consistency, simplicity and clarity, including by providing one set of overarching privacy principles (that is, the model UPPs);

- need to specify and modify the operation of the model UPPs in the context of credit reporting, including by providing requirements that are more and less stringent than those principles, as appropriate; and

- need to improve substantially the provisions regulating credit reporting—for example, to permit more comprehensive credit reporting[2] and to provide individuals with improved dispute resolution mechanisms.[3]

54.3 A desirable third tier of the regulatory model is a credit reporting code developed by industry with input from consumer groups and regulators, including the Office of the Privacy Commissioner (OPC) and the Australian Consumer and Competition Commission (ACCC). This code should provide detailed guidance within the framework provided by the Act and deal, for example, with a range of operational matters relevant to compliance with the permitted content, data quality and dispute resolution obligations set out in the regulations.

Part IIIA and the NPPs

54.4 In considering options for reform, it is important to understand the relationship between the credit reporting provisions and the existing National Privacy Principles (NPPs). Part IIIA of the *Privacy Act* was originally intended to adopt and reflect privacy principles in the specific context of credit reporting.[4] The NPPs were enacted

---

1 The model UPPs are discussed in Part D.
2 See Ch 55.
3 See Ch 59.
4 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

later, in 2000,[5] and established a set of general principles designed to provide privacy protection in respect of personal information in the private (non-government) sector.

54.5 The rules in Part IIIA are designed to achieve broadly the same objectives as the NPPs. The obligations in Part IIIA apply only in respect of credit reporting whereas the NPPs apply to the private sector generally. In substance, the provisions of Part IIIA of the *Privacy Act* constitute a third major set of privacy rules, in addition to the Information Privacy Principles (IPPs) and the NPPs—albeit more detailed and prescriptive than either of those sets of principles. For example, while NPP 1.1 sets out a general principle that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities, Part IIIA provides that a credit reporting agency must not include personal information in a credit information file unless the information comprises specified permitted content.[6]

54.6 The obligations in Part IIIA can be seen as both strengthening and derogating from the privacy protection afforded to personal information by the NPPs. A brief comparison of some of the NPPs and the credit reporting provisions illustrates this point.[7]

54.7 In some important respects, the NPPs can be seen as imposing a lower level of privacy protection than the provisions of Part IIIA:

- Under NPP 1, an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. This broad test of necessity can be contrasted with the detailed provisions of s 18E, which prescribe the permitted content of credit information files held by credit reporting agencies. Even if other categories of information can be shown to be necessary for credit reporting under NPP 1, collection is prohibited (even if the individual consents) under s 18E.

- Under NPP 2, an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection unless the secondary purpose is related to the primary purpose or within the reasonable expectations of the individual concerned. In addition, NPP 2.1(c) permits, in some circumstances, the use of information for the secondary purpose of direct marketing—including by related bodies corporate.[8] In contrast, ss 18K and 18N limit the disclosure of personal information by credit reporting

---

5 *Privacy Amendment (Private Sector) Act 2000* (Cth). The NPPs are located in *Privacy Act 1988* (Cth) sch 3.

6 *Privacy Act 1988* (Cth) s 18E(1).

7 The model UPPs do not depart significantly from the NPPs in these respects.

8 *Privacy Act 1988* (Cth) s 13B.

agencies and credit providers respectively to an exhaustive list of specific circumstances.

- Under NPP 3, an organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is 'up-to-date'.[9] There is no equivalent of s 18F, however, which provides for the deletion of personal information in credit information files after the end of maximum permissible periods for the keeping of different kinds of information.

- Under NPP 6, individuals have rights to access personal information about them. Unlike the equivalent rights under s 18H, NPP 6 specifically allows organisations to charge for access and contains an extensive list of exceptions, under which access may be refused in certain circumstances.

54.8 In other respects, the NPPs can be seen as imposing a higher level of privacy protection than the provisions of Part IIIA. Importantly, Part IIIA operates to authorise some information-handling practices that would not be permitted under the NPPs without the consent of the individual concerned:

- Sections 18K and 18N operate to authorise a range of secondary uses and disclosures of personal information that would not be permitted without consent under NPP 2.1—for example, credit reports may be used by mortgage insurers and those considering entering securitisation arrangements, without the individual's consent.[10]

- The credit reporting provisions implicitly permit indirect collection of personal information by credit reporting agencies while NPP 1.4 requires that, if it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

54.9 In this context, the Cyberspace Law and Policy Centre observed that Part IIIA departs from the usual rules relating to the use and disclosure of personal information (NPP 2), by allowing:

> (a) the bundling of use for assessing a credit application with disclosure for the secondary purpose of informing other credit providers via central credit reference databases;
>
> (b) a variation (distortion) of the normal meaning of consent; i.e. in this context it is not freely given with the option of withdrawal—rather it is merely an acknowledgement of a condition; and
>
> (c) the pooling of a multiplicity of bilateral information exchanges into a common centralised system, on economic efficiency grounds.[11]

---

9 A similar obligation applies to information in credit information files and credit reports: Ibid s 18G(a).
10 Ibid ss 18K(1)(ab), (ac), and (d).
11 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

54.10 A breach of a requirement of Part IIIA, unless the relevant provision states otherwise, has the same effect as a breach of one of the NPPs, and constitutes an 'interference with the privacy of an individual'.[12] Part IIIA and the NPPs operate independently.[13] Under s 13A(2), an organisation commits an interference with the privacy of an individual if it breaches a NPP, notwithstanding that the organisation is also a credit reporting agency or a credit provider. Section 16A(4) states that conduct that does not breach the NPPs is not lawful for the purposes of Part IIIA merely because it does not breach the NPPs.

Repeal and new regulation under the Act

54.11 There are three main approaches available for reform of the credit reporting provisions:

- Credit reporting could continue to be regulated under Part IIIA of the *Privacy Act 1988* (Cth) and its related provisions.

- Part IIIA and its related provisions could be repealed, and credit reporting regulated under the general provisions of the *Privacy Act*.

- Credit reporting could be regulated by new sectoral legislation dealing specifically with the privacy of credit reporting information.

54.12 There was little support in submissions for the retention of Part IIIA in its present form. As discussed in this chapter, even those who value the privacy protections provided by Part IIIA generally agreed that the provisions should be simplified, while retaining the basic rules.

54.13 The ALRC has concluded that the credit reporting provisions of the *Privacy Act* should be repealed and credit reporting governed by the general provisions of the Act and the model UPPs, supplemented by subordinate legislation. The reasons for this view include that the credit reporting provisions are an unjustified anomaly within the *Privacy Act*; the Act would be significantly simplified by the repeal of Part IIIA; the repeal of Part IIIA is consistent with the ALRC's recommendation that one set of privacy principles regulating both the public and private sectors be developed; and an equivalent level of privacy protection can be provided to individuals under the model UPPs and subordinate legislation.

---

12 See *Privacy Act 1988* (Cth) s 13(d).

13 A Tyree, 'The Privacy (Private Sector) Amendments' (2000) 11 *Journal of Banking and Finance Law and Practice* 313, 315.

The anomalous nature of Part IIIA

54.14 The credit reporting provisions are the only provisions in the *Privacy Act* that deal in detail with the handling of personal information within a particular industry or business sector. One credit reporting agency has observed that Part IIIA of the *Privacy Act* is a 'significantly more prescriptive legislative regime than applies to other arguably more sensitive sectors of the private sector'.[14] While it may be argued that credit reporting presents a suite of privacy issues that are uniquely deserving of specific regulation, the reasons for this anomaly are to some extent historical in that the credit reporting industry was made subject to privacy regulation before the rest of the private sector.

54.15 In 1990, when the credit reporting provisions were inserted into the *Privacy Act*, the Act had very limited application to the private sector.[15] While further privacy regulation was anticipated,[16] comprehensive coverage of the private sector was not implemented until 2000, with the enactment of the *Privacy Amendment (Private Sector) Act 2000* (Cth). The *Privacy Amendment (Private Sector) Act*, which came into effect on 21 December 2001, established the NPPs, which apply to the handling of personal information in the private sector.

54.16 The history of credit reporting regulation in Australia may be contrasted with that in New Zealand where credit reporting regulation, under a legally binding code, followed the enactment of the *Privacy Act 1993* (NZ)—which applied information privacy principles across the public and private sectors.

54.17 As discussed in Chapter 18, the ALRC recommends that the IPPs and NPPs should be replaced by a single set of privacy principles regulating both the public and private sectors (the model UPPs). The repeal of Part IIIA is consistent with the development of one set of legislative privacy principles[17] and with the approach taken to the privacy protection of health information.[18]

The need for specific credit reporting regulation

54.18 The credit reporting provisions of the *Privacy Act* are complex and prescriptive. While some of this complexity and prescriptiveness may be unnecessary, effective regulation of credit reporting needs to incorporate at least some of this detail and, more generally, to tailor broad privacy principles to the specific conditions of the credit reporting industry.

---

14 Baycorp Advantage, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 16 March 2005.

15 The *Privacy Act* provided guidelines for the collection, handling and use of individual tax file number information in the private, as well as public, sector: *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).

16 For example, the second reading speech stated that the credit reporting provisions were 'the next step' in the Government's program to introduce comprehensive privacy protection: Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

17 See Ch 4.

18 See Part H.

54.19 Incorporating the credit reporting provisions into regulations or a code under the *Privacy Act*, rather than leaving them in the primary legislation, makes it easier for rules to be amended to take into account the changing nature of the credit sector in Australia and developments in the role and potential uses of the credit reporting system.

54.20 One approach might be to incorporate the credit reporting provisions into a legally binding code issued by the Privacy Commissioner. Models of credit reporting privacy codes include those in New Zealand[19] and Hong Kong.[20] In New Zealand, credit reporting is regulated under a legally binding code issued by the Privacy Commissioner under the Act.[21] Many basic elements of the *Credit Reporting Privacy Code 2004* (NZ) are similar, in effect, to regulation in Australia.

Sectoral credit reporting legislation

54.21 An alternative approach to reform of the credit reporting provisions of the *Privacy Act* would be to repeal those provisions and enact new sectoral legislation dealing with the privacy of credit reporting information.[22] Sectoral credit reporting legislation might deal with related consumer protection issues and be designed to operate consistently with the *Consumer Credit Code*,[23] or incorporated into the Code. One advantage of such an approach would be to consolidate a link between regulation of credit reporting and the responsible lending and related obligations of credit providers.[24]

54.22 The possible disadvantages include the following:

- Banks, finance companies, other credit providers and consumers would have to deal with two statutory privacy regimes—that is, specific rules in relation to credit reporting, and the model UPPs in relation to other aspects of handling personal information.

- Specific credit reporting legislation may add to problems caused by inconsistency and fragmentation in privacy law, including complexity of privacy regulation, varying levels of privacy protection, and regulatory gaps.

---

19 *Credit Reporting Privacy Code 2004* (NZ).

20 Office of the Privacy Commissioner for Personal Data Hong Kong, *Code of Practice on Consumer Credit Data* (1998).

21 *Credit Reporting Privacy Code 2004* (NZ) under *Privacy Act 1993* (NZ) s 46.

22 In this Report, the term 'credit reporting information' is used to describe all personal information recommended to be covered by the *Privacy (Credit Reporting Information) Regulations*.

23 The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories.

24 The concept of responsible lending and its relationship with credit reporting is discussed in Ch 55.

54.23 If credit reporting regulation were to be located outside the Act, questions may arise about whether the Privacy Commissioner remains the appropriate regulator.[25] For example, credit reporting conceivably could be regulated as a financial services consumer protection law by the Australian Securities and Investments Commission (ASIC).

54.24 Overseas jurisdictions take differing approaches to the location of credit reporting legislation and the nature of the regulator. Most commonly, however, credit reporting is regulated within privacy law regimes, except where regulation of credit reporting preceded the enactment of privacy laws, or where there is no comprehensive privacy or data protection legislation.[26]

54.25 In the United States, credit reporting is regulated under the *Fair Credit Reporting Act 1970* (US) by the Federal Trade Commission.[27] In the United Kingdom, the activities of credit reference agencies are regulated by both the *Consumer Credit Act 1974* (UK) and under privacy legislation.[28] New Zealand and Canada more closely follow the Australian model. Credit reporting is regulated by these jurisdictions' privacy commissioners under the *Privacy Act 1993* (NZ) and the *Personal Information Protection and Electronic Documents Act 2000* (Canada) respectively.

Discussion Paper proposals

54.26 In the Discussion Paper *Review of Australian Privacy Law* (DP 72), the ALRC stated that the repeal of Part IIIA need not result in any lessening of privacy protection in relation to credit reporting. It would not be sufficient, however, to leave credit reporting to be regulated by the model UPPs alone, or by the UPPs supported by a binding code issued by the Privacy Commissioner. The reasons included that:

- credit reporting regulation needs to be able to impose more *or* less stringent obligations on credit reporting agencies and credit providers than are provided for in the UPPs;[29]

- credit reporting requires a level of prescription, beyond the principles-based approach of the UPPs, to ensure that credit reporting agencies, credit providers and individuals understand their obligations and rights; and

---

25 The OPC already has some functions under legislation other than the *Privacy Act* including the *Data-matching Program (Assistance and Tax) Act 1990* (Cth); *National Health Act 1953* (Cth); *Telecommunications Act 1997* (Cth); and *Crimes Act 1914* (Cth): see Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).

26 Veda Advantage, *Submission PR 272*, 29 March 2007.

27 The United States does not have a federal information privacy commissioner.

28 The United Kingdom Information Commissioner (the equivalent of the OPC) deals with credit reporting complaints, and credit reference agencies are bound by the *Data Protection Act 1998* (UK).

29 As discussed above, Part IIIA currently imposes obligations on credit reporting agencies and credit providers that are both more *and* less stringent than those provided by the NPPs.

- derogation from the UPPs would not be permitted under the ALRC's proposed approach to codes under the *Privacy Act*.[30]

54.27 Accordingly, in DP 72, the ALRC proposed that:

- the credit reporting provisions of the *Privacy Act* should be repealed and credit reporting regulated under the general provisions of the Act and the model UPPs;[31] and

- privacy rules, which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information, should be promulgated in regulations.[32]

54.28 The ALRC also proposed that the:

- obligations imposed on credit reporting agencies and credit providers by the proposed *Privacy (Credit Reporting Information) Regulations* should be in addition to those imposed by the proposed UPPs;[33] and

- regulations should be drafted to contain only those requirements that are different or more specific than are provided for in the proposed UPPs.[34]

Submissions and consultations

54.29 Support for the review and reform of credit reporting regulation was expressed throughout the course of the Inquiry, by consumer and industry groups. These views are discussed below.

---

30 The ALRC proposed that binding privacy codes should provide guidance or standards that contain obligations that are at least equivalent to those under the Act: Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–9.

31 Ibid, Proposal 50–1.

32 Ibid, Proposal 50–2.

33 Ibid, Proposal 50–3.

34 Ibid, Proposal 50–4.

Repeal of Part IIIA

54.30 There was substantial support for the repeal of Part IIIA.[35] The credit reporting provisions were criticised for being overly complex and prescriptive. Part IIIA was characterised as being 'inflexible, difficult to work with and poorly suited to both consumer protection and efficient business objectives'.[36]

54.31 While some stakeholders appeared to support the retention of Part IIIA,[37] some of these stakeholders also favoured substantial modification of the current regulatory scheme—for example, by consolidating Part IIIA, the *Credit Reporting Code of Conduct* and the Privacy Commissioner's credit provider determinations[38] into one body of provisions.[39]

54.32 There was little support for new credit reporting legislation enacted outside the *Privacy Act*. The OPC noted that regulating credit reporting as an industry rather than regulating the handling of personal information used in credit reporting would create 'further inconsistency and fragmentation in Australian privacy law'.[40] Other stakeholders also expressed concern about fragmentation in privacy law.

54.33 The Australasian Retail Credit Association (ARCA), for example, stated that maintaining the OPC as the sole regulator in relation to credit reporting would 'help ensure the consistency of policy decision making and reduced complexity'—especially given that the credit industry is a 'highly regulated sector with compliance to multiple regulations requiring careful consideration to limit duplication and management confusion'.[41] Conversely, some stakeholders suggested that ASIC might be a more effective credit reporting regulator.[42] The reasons for this view included the close

---

35 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Abacus–Australian Mutuals, *Submission PR 456*, 11 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Australian Finance Conference, *Submission PR 294*, 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007; Australian Institute of Credit Management, *Submission PR 224*, 9 March 2007.

36 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

37 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Optus, *Submission PR 258*, 16 March 2007.

38 Under *Privacy Act 1988* (Cth) s 11B.

39 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

40 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

41 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

42 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; National Legal Aid, *Submission PR 265*, 23 March 2007.

connections between credit reporting regulation and the way credit is provided and debts pursued,[43] and more general concerns about the effectiveness of the OPC as a regulator.[44]

Regulations or code

54.34 Stakeholders generally accepted that privacy protection in credit reporting should not rely on general privacy principles alone, but needs to be supported by regulations or a legally binding code (or both).[45] There were some exceptions. Telstra, for example, objected to the imposition of obligations beyond those provided by the UPPs. Telstra encouraged the ALRC to 'consider whether the new, comprehensive UPPs could be broad enough in scope to cover all aspects of privacy (including credit related issues), which would eliminate the need for separate regulations'.[46]

54.35 For most stakeholders, however, the key concerns revolved around the appropriate location of credit reporting regulation. Some industry stakeholders continued to express a preference for implementing new credit reporting rules through a code,[47] developed by industry and approved by the OPC, rather than by regulations, made by the Governor-General in Council on the recommendation of the responsible Minister.

54.36 The Australian Finance Conference (AFC), for example, stated that, while it supported the overall approach to reform proposed by the ALRC in DP 72, a code should be used rather than regulations. The code should be 'developed collaboratively with industry, consumer representatives and government' and cover 'both matters of policy and operational issues'.[48] The OPC favoured setting out credit reporting privacy rules 'in a binding credit code issued by the Privacy Commissioner as a legislative

---

43 National Legal Aid, *Submission PR 265*, 23 March 2007.

44 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

45 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; Veda Advantage, *Submission PR 272*, 29 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007.

46 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. Telstra added, however, that any 'credit specific obligations, and only to the extent that they are absolutely necessary, should be imposed by legislation'.

47 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

48 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

instrument'. The OPC accepted, nevertheless, that regulations would be a viable alternative approach.[49]

54.37 ARCA accepted that regulations may be desirable to 'facilitate actions that may be otherwise broader than contemplated by the UPPs' and to 'provide a framework for credit reporting outcomes and impose specific obligations and constraints on credit providers and CRAs'. ARCA was concerned, however, that the regulations, while supplementing the UPPs:

> should not contain a level of detail that would result in rigid and prescriptive rules that rapidly date and impede innovation. It is proposed that the rules underpinning the regulations have flexibility to support an industry operating in a climate of evolving technology and that would be supported by a code of conduct approach.[50]

54.38 ARCA suggested that, in general, the content of the regulations should be limited to those matters that are 'unlikely to change with market conditions' and should be outcome-based rather than prescribe how outcomes are to be achieved. In its submission, ARCA nevertheless accepted the idea that privacy rules for credit reporting should be promulgated in regulations under the *Privacy Act*.[51]

54.39 ARCA's position was explicitly supported in other submissions[52] and other stakeholders also favoured regulations.[53] ARCA recommended a three-tiered regulatory structure, broadly consistent with that proposed by the ALRC in DP 72, and comprising:

- the privacy principles contained in the *Privacy Act*;
- regulations to provide a framework for regulating credit reporting under the Act, modify the privacy principles where necessary and set out the additional obligations of credit providers and credit reporting agencies; and
- a code of conduct that provides detailed policies and procedures for credit reporting.

---

49 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

50 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

51 Ibid.

52 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Westpac, *Submission PR 472*, 14 December 2007; Abacus–Australian Mutuals, *Submission PR 456*, 11 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007.

53 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

54.40 Galexia recommended a similar regulatory framework for credit reporting, comprising general principles, detailed regulations, and industry operating rules.[54] This basic framework was also supported, with some qualifications about the content and location of various provisions, by some other stakeholders.[55]

54.41 Concerns were expressed, however, that current privacy protections should not be downgraded by the repeal of Part IIIA and its replacement with the *Privacy (Credit Reporting Information) Regulations*. The Cyberspace Law and Policy Centre suggested, for example, that the starting point for any review of the credit reporting provisions should be 'an acknowledgement that the current centralised credit reporting systems represent a privileged state-sanctioned exception from normal expectations of privacy'.

> From this starting point, it is only to be expected that there should be strict controls, limits and additional safeguards, and the onus should be on the community of lenders to justify any weakening of controls; derogations from obligations, or extension of the privilege in the form of more comprehensive credit reporting.[56]

Relationship between the UPPs and the regulations

54.42 By proposing that the obligations imposed by the new *Privacy (Credit Reporting Information) Regulations* should be 'in addition to' those imposed by the UPPs,[57] the ALRC intended to indicate that a credit provider or credit reporting agency would need to comply with both the model UPPs and the regulations, which would modify the operation of the UPPs in particular contexts. This overall approach met with broad agreement from stakeholders.[58]

54.43 An alternative approach is taken in New Zealand under the *Credit Reporting Privacy Code 2004* (NZ) (NZ Code).[59] The *Privacy Act 1993* (NZ) provides that the doing of any action that would otherwise be a breach of an information privacy principle[60] is deemed not to be a breach if the action is done in compliance with the NZ

---

54 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.

55 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

56 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

57 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–3.

58 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

59 *Credit Reporting Privacy Code 2004* (NZ). The NZ Code is a binding code issued by the Privacy Commissioner pursuant to the *Privacy Act 1993* (NZ).

60 The information privacy principles are the NZ equivalent of the NPPs and IPPs.

Code.[61] General requirements of the information privacy principles are incorporated into the credit reporting rules set out in the NZ Code, along with those that are different or more specific than provided for in the principles.

54.44 Stakeholders did not call for such an approach in Australia. Rather, it was suggested that credit reporting regulations should not duplicate the obligations set out in general privacy principles.[62]

Approaches to drafting the regulations

54.45 Stakeholders referred to the need to simplify credit reporting regulation.[63] The Consumer Credit Legal Centre (NSW) (CCLC), for example, stated:

> The drafting of the current Part IIIA is complex, rigid and often difficult to comprehend and apply. It also arguably undermines the thrust of the privacy principles. Credit providers, consumers and decision-makers alike become mired in the detailed requirements of the Act and can easily lose sight of the principles those sections were meant to uphold.[64]

54.46 National Legal Aid suggested that while some of the complexity of Part IIIA would have been difficult to avoid,[65] 'there is now an opportunity to prune back some of this complexity, given the broader application of the *Privacy Act*, changes in the way credit is provided and the enhanced capacity of computerised information systems'.[66]

54.47 Industry stakeholders made similar comments. AAPT, for example, stated that the credit reporting provisions 'need to be re-written in plain English and in a simple style' and that the provisions are 'currently difficult to read and consumer protection must therefore be eroded'.[67] Telstra stated that any 'new credit specific rules require careful drafting to avoid the interpretative difficulties and lack of clarity now existing in complying with Part IIIA'.[68]

---

61 *Privacy Act 1993* (NZ) s 53(a). On the other hand, failure to comply with the Code, even though that failure is not otherwise a breach of any information privacy principle, is deemed to be a breach of an information privacy principle: s 53(b).

62 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.

63 See, eg, N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Optus, *Submission PR 258*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Mortgage and Finance Association of Australia, *Submission PR 231*, 9 March 2007; AAPT Ltd, *Submission PR 87*, 15 January 2007.

64 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 67.

65 Given the need, among other things, to establish a firm constitutional basis for regulating consumer credit and avoid unforseen consequences to the finance industry of restricting access to credit reporting information: National Legal Aid, *Submission PR 265*, 23 March 2007.

66 Ibid.

67 AAPT Ltd, *Submission PR 87*, 15 January 2007.

68 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

ALRC's view

54.48 A degree of consensus emerged around the overall approach that should be taken to the future regulation of credit reporting, based on that proposed by the ALRC in DP 72. The starting point is that Part IIIA should be repealed and credit reporting governed by the general provisions of the Act and the model UPPs, supplemented by subordinate legislation or a code.

54.49 This approach is consistent with the ALRC's overall approach to reform of the *Privacy Act*. As discussed in detail in Chapter 4, the ALRC does not recommend the adoption of a pure form of principles-based regulation. Rather, the ALRC takes a pragmatic approach, adopting what could be described as a hybrid model. The model draws significantly on principles-based regulation as its foundation, but allows for a reversion to more traditional rules-based regulation where appropriate. Subordinate legislation can be introduced to provide greater specificity and certainty in regulating privacy in relation to particular activities—including credit reporting.

Regulations or code

54.50 On the issue of regulations or a code, the ALRC recommends that the primary source of privacy rules imposing obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information, should be regulations promulgated under the *Privacy Act*.

54.51 Consistently with the ALRC's overall approach to reform of the *Privacy Act*, the *Privacy (Credit Reporting Information) Regulations* would be more detailed and specific than the UPPs and derogate from the requirements in the privacy principles, by providing different (that is, more or less stringent) requirements than are provided for in the principles.[69]

54.52 This approach is dictated, in part, by the ALRC's recommendations in relation to the development and issuing of codes of conduct under Part IIIAA of the *Privacy Act*.[70] In this context, the ALRC recommends that privacy codes approved under Part IIIAA should not replace the obligations provided by the UPPs and must impose obligations that are at least equivalent to those under the Act.[71]

54.53 Some industry stakeholders favoured a code rather than regulations as the regulatory mechanism, although they did not always specify the desired legal status of

---

69 The ALRC recommends, in Ch 5, that the regulation-making power in the *Privacy Act* provide expressly that regulations may modify the operation of the UPPs to impose more or less stringent requirements: See Rec 5–1.

70 The code-making power under Part IIIAA of the *Privacy Act* is discussed in detail in Ch 48.

71 Rec 48–1.

such a code.[72] To provide effective regulation of credit reporting, a statutory basis for a code (whether issued by the OPC or some other body) would be required to ensure its obligations are binding on all participants in the credit reporting industry. The reasons for preferring a code included: perceptions that the process for developing codes would be more 'industry-driven'; and that codes are more easily amended, for example, to take account of changes in industry practices or technology.

54.54 A statutory code-making power could be drafted to allow the OPC to issue codes that derogate from the model UPPs, in the way permissible under the ALRC's recommended regulation-making power.[73] The ALRC considers, however, that even if the same result, in terms of privacy protection, might be achieved through a code issued by the OPC, it is more appropriate to recommend the promulgation of regulations by the responsible Minister.

54.55 As discussed in Chapter 4, this approach better conforms with the principles of responsible government and parliamentary supremacy, by clearly vesting in Parliament the power to control the rules that apply to privacy. Proceeding by way of regulations also is consistent with the ALRC's approach to the privacy of health information.

Relationship between the UPPs and the regulations

54.56 As discussed above, the content of the *Privacy (Credit Reporting Information) Regulations* will include provisions that can be seen as both strengthening and lessening the privacy protection afforded to personal information by the model UPPs. For example, the *Privacy (Credit Reporting Information) Regulations* will continue to limit the permitted content of credit reporting information held by credit reporting agencies and will mandate the indirect collection of personal information.

54.57 The relationship between the model UPPs and the new *Privacy (Credit Reporting Information) Regulations* requires consideration in light of the potential inconsistencies. Two broad approaches appear available.

- The relationship between the UPPs and the *Privacy (Credit Reporting Information) Regulations* could mirror the existing relationship between the NPPs and Part IIIA of the *Privacy Act*. Credit reporting agencies and credit providers would have to comply with both regimes.

- Alternatively, the requirements of the UPPs could be incorporated into the regulations, along with those that are different or more specific than provided for in the UPPs. A breach of the UPPs would be deemed not to be a breach if done in compliance with the credit reporting regulations.[74]

---

72 See, eg, Australian Finance Conference, *Submission PR 398*, 7 December 2007.
73 Rec 5–1.
74 That is, following the model provided by the NZ Code.

54.58 Credit reporting agencies and credit providers should have to comply with both the model UPPs and the *Privacy (Credit Reporting Information) Regulations*. This approach is consistent with the existing relationship between the credit reporting provisions and general privacy principles contained in the *Privacy Act*, and with the approach to be taken to the new *Privacy (Health Information) Regulations*.[75]

54.59 The regulations should be drafted to contain only those requirements that are different or more specific than provided for in the UPPs. Any problems of inconsistency would be limited because conduct that complies with the *Privacy (Credit Reporting Information) Regulations* is 'required or authorised by law' under the model UPPs.

Approaches to drafting the regulations

54.60 The existing credit reporting provisions contained in Part IIIA and associated provisions should be recast as regulations under the *Privacy Act*, incorporating content that reflects the policy recommendations resulting from the current Inquiry. Such is the complexity of the provisions, and the definitions in particular, that there would be good reason for redrafting them, even if the substance of regulation were to remain largely unchanged.

54.61 In drafting the *Privacy (Credit Reporting Information) Regulations*, the existing provisions of Part IIIA of the *Privacy Act* remain an appropriate starting point. Despite the criticisms made of the existing credit reporting provisions, Part IIIA of the Act provides comprehensive privacy protection. Further, the current practices of credit reporting agencies and credit providers have been developed to comply with these obligations:

> Significant resources have been expended to ensure documentation, procedures and training meet the requirements of Part IIIA and related provisions on an on-going basis … Any change would potentially impact and bring with it significant cost which may be borne by customers in the pricing of credit products.[76]

54.62 In the interests of maintaining privacy protection and minimising the transition costs to industry of new credit reporting regulations, significant departures from the policy framework of Part IIIA need to be justified.

54.63 There is potential for the *Privacy (Credit Reporting Information) Regulations* to simplify significantly the privacy rules relating to credit reporting. A number of approaches could be pursued. There is room, for example, to simplify the overall regulatory framework by consolidating the provisions of Part IIIA, the Privacy

---

75 See Part H.

76 Australian Finance Conference, *Submission PR 294*, 18 May 2007.

Commissioner determinations and the *Credit Reporting Code of Conduct*[77]—notably in relation to the definition of credit provider (discussed below).

54.64 In addition, some of the drafting approaches taken in the NZ Code may have the potential to simplify credit reporting regulation in Australia. The NZ Code was significantly influenced by the existing Australian credit reporting provisions and intended to bring about 'greater trans-Tasman regulatory alignment'.[78] The New Zealand Assistant Privacy Commissioner has summarised the NZ Code as taking a similar approach to Part IIIA on some broad issues[79] and in some specific matters,[80] while being less complex and prescriptive.[81] There are, however, notable differences in some areas, including in relation to limits on the disclosure of credit information, which are less restrictive in New Zealand.[82]

54.65 The relative simplicity of the NZ Code can be illustrated by the differing approaches to the drafting of the provisions dealing with the use and disclosure of credit information.[83] The NZ Code is able to deal succinctly with limits on use and disclosure of credit information by credit reporters in Rules 10 and 11 respectively, while Part IIIA of the *Privacy Act* relies on the extensive provisions of ss 18K, 18L, 18N, 18P and 18Q.[84]

54.66 More generally, the drafting and layout of the credit reporting provisions could be improved to assist credit providers, credit reporting agencies and consumers to understand their obligations and rights.[85] ARCA agreed, for example, that there is 'value in leveraging' aspects of the NZ Code and the existing provisions of Part IIIA. Many of the recommendations made in this and subsequent chapters should contribute to a less complex form of credit reporting regulation.

---

77 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

78 New Zealand Government Privacy Commissioner, *Credit Reporting Privacy Code: Frequently Asked Questions* (2006) <www.privacy.org.nz/privacy-act/frequently-asked-questions> at 5 May 2008.

79 For example, in relation to the information a credit reporting agency is permitted to collect.

80 For example, the definition of 'serious credit infringement'.

81 B Stewart, 'Credit Reporting Privacy Code 2004' (Paper presented at New Zealand Credit & Finance Institute, Auckland, 21 February 2005).

82 For example, a credit reporter may disclose credit information to a prospective landlord or employer: *Credit Reporting Privacy Code 2004* (NZ), Rule 11(2).

83 Some of this simplicity results from that fact that, in New Zealand, the credit reporting activities of credit providers are regulated indirectly through obligations imposed under contract. Under the NZ Code, a credit reporter must ensure that a complying subscriber agreement is in place before disclosing any credit information to a credit provider: see Ibid, Rules 5(2)(d); 8(3)(a); 11(2) and sch 3. The handling of credit information disclosed to a credit provider by a credit reporter is covered by the general information privacy principles of the *Privacy Act 1993* (NZ), as it would be if the information was obtained by the credit provider from its own clients directly. There was no call for such an approach in Australia.

84 The NZ Code deals with the use and disclosure of credit information in less than 1,000 words, as compared to the 6,000 relevant words of Part IIIA (leaving aside related definitions).

85 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

54.67 It must be stressed, however, that it is not the ALRC's practice to draft regulations. As discussed in Chapter 1, this is partly because drafting is a specialised function better left to the legislative drafting experts and partly a recognition that the ALRC's time and resources are better directed towards determining the policy that will shape any resulting legislation.

Recommendation 54–1 The credit reporting provisions of the *Privacy Act* should be repealed and credit reporting regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles, and regulations under the *Privacy Act*—the new *Privacy (Credit Reporting Information) Regulations*—which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information.

Recommendation 54–2 The new *Privacy (Credit Reporting Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model Unified Privacy Principles.

Application of the regulations

54.68 The scope of Part IIIA of the *Privacy Act* is determined, in large part, by definitions of:

- 'credit information files', 'credit reports' and 'reports';
- 'credit reporting agency'; and
- 'credit provider'.

54.69 The following part of this chapter discusses issues concerning the scope of the new *Privacy (Credit Reporting Information) Regulations*, with reference to these existing definitions. The ALRC makes recommendations with regard to equivalent provisions of the new regulations. The finer detail of drafting and decisions about whether the definitions are best placed in the *Privacy Act* itself or in the regulations are matters for the Australian Government to resolve, with the assistance of the Office of Parliamentary Counsel.

Credit reporting information

54.70 The provisions of Part IIIA apply variously to personal information in 'credit information files', 'credit reports' and 'reports'. As discussed in Chapter 53, each term is defined differently. Briefly:

- a 'credit information file' is information kept by a credit reporting agency in the course of carrying on a credit reporting business;[86]

- a 'credit report' is information prepared by a credit reporting agency that is used (by a credit provider) in establishing an individual's eligibility for credit;[87] and

- a 'report' is a credit report or any other information that has any bearing on an individual's credit worthiness.[88]

54.71 Stakeholders questioned the need to retain these separate terms, especially in view of commercial practice and technology.[89] Veda Advantage noted that the terms are 'out of step with commercial practice, technology and market demand' given that the use of 'data streams within the credit environment has meant that the traditional concept of a physical credit report no longer exists'.[90]

Discussion Paper proposal

54.72 In DP 72, the ALRC proposed that the *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'. The existing definitions of 'credit information files', 'credit reports' and 'reports' would not need to be reproduced in the new regulations.

54.73 The ALRC did not favour incorporating a broader definition of credit information based on the definition of 'report' in s 18N(9), as suggested by some stakeholders.[91] Section 18N applies to information contained in 'reports relating to credit worthiness'. A 'report' is defined, for the purposes of the section, as

> (a) a credit report; or
>
> (b) … any other record or information, whether in a written, oral or other form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity;
>
> but does not include a credit report or any other record or information in which the only personal information relating to individuals is publicly available information.[92]

---

86 *Privacy Act 1988* (Cth) s 6(1).
87 Ibid s 6(1).
88 Ibid s 18N(9).
89 Australian Finance Conference, *Submission PR 294*, 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Veda Advantage, *Submission PR 272*, 29 March 2007.
90 Veda Advantage, *Submission PR 272*, 29 March 2007.
91 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.
92 *Privacy Act 1988* (Cth) s 18N(9).

54.74 A 'credit report' is defined as

> any record or information, whether in a written, oral or other form, that:
>
> (a) is being or has been prepared by a credit reporting agency; and
>
> (b) has any bearing on an individual's:
>
> (i) eligibility to be provided with credit; or
>
> (ii) history in relation to credit; or
>
> (iii) capacity to repay credit; and
>
> (c) is used, has been used or has the capacity to be used for the purpose of serving as a factor in establishing an individual's eligibility for credit.[93]

54.75 Rather, the ALRC's view was that the proposed definition of credit reporting information should combine elements of the current definitions of 'credit information file' and 'credit report'. The ALRC suggested the following illustrative definition:

> ***credit reporting information***, means any record that contains personal information about an individual and is:
>
> (a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or
>
> (b) held by a credit provider and:
>
> (i) is being or has been prepared by a credit reporting agency; and
>
> (ii) has any bearing on an individual's eligibility to be provided with credit, history in relation to credit, or capacity to repay credit; and
>
> (iii) is used, has been used or has the capacity to be used for the purpose of serving as a factor in establishing an individual's eligibility for credit.[94]

Submissions and consultations

54.76 There was broad agreement, at least in principle, with the ALRC's proposal that the *Privacy (Credit Reporting Information) Regulations* should apply to a new category of personal information, to be defined as 'credit reporting information'.[95] Stakeholders expressed a range of concerns, however, about the potential breadth of the proposed definition.

---

93 Ibid s 6(1).

94 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [50.87].

95 GE Money Australia, *Submission PR 537*, 21 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

54.77 ARCA stated that the definition of credit reporting information should only encompass information about credit worthiness. ARCA noted that

> organisations that operate credit reporting businesses use and disclose some types of personal information (especially that drawn from public registers) for multiple purposes, only one of which is credit reporting …[96]

54.78 ARCA stated that, unless the definition is focused on 'credit worthiness', additional costs would be imposed on credit reporting agencies 'as they would need to maintain multiple copies of data bases to ensure that these categories of information could be used in non-credit circumstances'.[97] Similarly, Veda Advantage suggested that credit reporting information should cover only 'a record containing personal information related to an individual's credit worthiness' that is either: held and maintained by a credit reporting business; or prepared by a credit reporting business and held by a credit provider and used to assess eligibility for credit.[98]

54.79 More generally, industry stakeholders expressed concern that the definition of credit reporting information should ensure that the regulations cover only consumer, as opposed to commercial, credit reporting information and do not cover publicly available information.[99]

54.80 Other stakeholders considered that the new *Privacy (Credit Reporting Information) Regulations* should also apply to a broad category of information similar to that covered by existing s 18N of the *Privacy Act*—that is, information with any bearing on an individual's credit worthiness regardless of its source.[100] Section 18N is discussed in Chapter 57.

ALRC's view

54.81 A workable definition of credit reporting information is critical to the coverage of the new *Privacy (Credit Reporting Information) Regulations* and the formulation of the ALRC's recommendations. The ALRC's recommendations are based on the assumption that 'credit reporting information' comprises a subset of 'personal information', as the latter term is defined in the *Privacy Act*; and that the *Privacy (Credit Reporting Information) Regulations* apply only to credit reporting information.

---

96 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

97 Ibid. Especially given ARCA's recommendation that 'credit reporting information' be subject to a regulated primary purpose: See Ch 57.

98 Veda Advantage, *Submission PR 498*, 20 December 2007.

99 Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. Telstra considered that the definition should be 'more clearly and strictly confined to credit information files held by credit reporting agencies, and credit reports that they provide': Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

100 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

54.82 The desirable content of the definition was canvassed in many different contexts. The ALRC understands industry concerns about the need to ensure the definition of credit reporting is not inappropriately broad. On the other hand, limiting the coverage of the regulations to personal information that is 'about credit worthiness', however defined, risks providing incomplete privacy protection for consumers.

54.83 This is because some personal information used in credit assessment processes cannot be said to be 'about credit worthiness' in any real respect. As discussed in Ch 52, when credit providers assess an individual's eligibility for credit, credit scoring is often used. Credit scoring involves the use of mathematical algorithms or statistical programs that assign a credit score to an individual based on information derived from a number of sources. That information may be obtained from credit reports, the credit application or the credit provider's own records. In Australia, credit scoring systems used by individual credit providers are often referred to as 'scorecards'.

54.84 Credit scorecards used by Australian credit providers incorporate a range of information that is considered predictive of credit risk. Data items such as age; state of residence; possession of a driver's licence; category of employment and time at current employment; residential status (renting, subject to mortgage, ownership etc); and time at current and previous addresses is commonly incorporated into scorecards. The possession of a driver's licence, for example, is considered a positive factor in assessing eligibility for credit. It is difficult, however, to interpret this information as being information 'about' credit worthiness. Rather, there is a statistical relationship between this characteristic and credit worthiness in the models developed by credit providers.

54.85 The ALRC is concerned that, if the definition of credit reporting information is too closely linked to credit worthiness, some items of personal information disclosed by credit reporting agencies to credit providers would not receive the additional protection of the *Privacy (Credit Reporting Information) Regulations* in relation to, for example, access, correction and dispute resolution. In the ALRC's view, the point is to regulate the handling of information that is maintained by credit reporting agencies and used by credit providers to establish an individual's eligibility for credit.

54.86 The ALRC recommends that the definition of 'credit reporting information' should include only personal information that is maintained or prepared by a credit reporting agency or, having been prepared by an agency, is held by a credit provider and is used, or is capable of being used, for the purpose of establishing an individual's eligibility for credit. The following definition is an appropriate starting point:

> ***credit reporting information***, means any record that contains personal information about an individual and is:
>
> (a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or

(b) held by a credit provider and:

(i) has been prepared by a credit reporting agency; and

(ii) is used, has been used or has the capacity to be used for the purpose of serving as a factor in establishing an individual's eligibility for credit.

Recommendation 54–3 The new *Privacy (Credit Reporting Information) Regulations* should apply only to 'credit reporting information', defined for the purposes of the new regulations as personal information that is:

(a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or

(b) held by a credit provider; and

(i) has been prepared by a credit reporting agency; and

(ii) is used, has been used or has the capacity to be used in establishing an individual's eligibility for credit.

Credit reporting agencies

54.87 Under the *Privacy Act*, 'a person is a credit reporting agency if the person is a corporation that carries on a credit reporting business'.[101] A 'credit reporting business' is defined as

> a business or undertaking … that involves the preparation or maintenance of records containing personal information relating to individuals (other than records in which the only personal information relating to individuals is publicly available information), for the purpose of, or for purposes that include as the dominant purpose the purpose of, providing to other persons (whether for profit or reward or otherwise) information on an individual's:
>
> (a) eligibility to be provided with credit; or
>
> (b) history in relation to credit; or
>
> (c) capacity to repay credit;
>
> whether or not the information is provided or intended to be provided for the purposes of assessing applications for credit.[102]

Discussion Paper proposal

54.88 The OPC recommended that the definition of a 'credit reporting business' should be amended to remove the exclusion 'other than records in which the only

101 *Privacy Act 1988* (Cth) s 11A.
102 Ibid s 6(1).

personal information relating to individuals is publicly available information'. The OPC stated that this would have the effect of regulating publicly available personal information collected by a credit reporting agency for credit assessment purposes under Part IIIA, rather than the NPPs.

> The Office believes that all relevant types of personal information should be regulated by Part IIIA if they are made available to banks and financial institutions in assessing an individual's eligibility to be provided with credit, indicate their credit history or capacity to repay credit. Moreover, a credit provider may have no obligations to comply with the NPPs if they are a small business operator within the meaning of s 6D. The effect will be that the provisions of Part IIIA will regulate this activity not the NPPs.[103]

54.89 Consistently with this view, the ALRC, in DP 72, proposed that the definition of a 'credit reporting business', if based on that in s 6(1) of the *Privacy Act*, should exclude the phrase 'other than records in which the only personal information relating to individuals is publicly available information'.[104]

Submission and consultations

54.90 ARCA agreed in principle with the ALRC's proposal.[105] Other stakeholders also supported the proposal, subject to qualifications about the coverage of commercial credit information and publicly available information.[106]

54.91 The ALRC proposal may, however, have been understood in different ways by stakeholders. This is perhaps unsurprising, as the words proposed to be excluded constitute an exception within the definition of a 'credit reporting business'. This definition is itself a component of the definitions of 'credit reporting agency', 'credit information file' (and the ALRC's proposed definition of 'credit reporting information').

54.92 ARCA suggested that the regulations should provide a new definition of 'credit reporting agency'. A credit reporting agency should, in ARCA's view, be defined as 'an organisation that carries on a business or undertaking that involves the preparation or maintenance of records containing personal information for the dominant purpose of, providing to other persons information on an individual's credit worthiness'. ARCA

---

103 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

104 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–6.

105 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

106 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

was concerned that publicly available information held by a credit reporting agency not be regulated as credit reporting information simply by virtue of that fact.[107]

54.93 Veda Advantage also expressed concern about the possible extension of credit reporting regulation to publicly available information generally, where held by a credit reporting agency.

> Such an extension is inconsistent with the objective of simplifying privacy laws. It imposes additional obligations on the handling of publicly available data that are specific to the credit reporting business—with additional costs—without any proportional benefit to protecting the privacy of individuals. It would mean any public information used at any point by a credit reporting agency—including responding to a public access request—would be credit reporting information. Accordingly, it would be limited by the primary purpose of credit reporting information, meaning it could not be used for any other purpose.[108]

54.94 Veda stated that to have the same data set covered by different rules (depending on the business holding it) would lead to 'unnecessary confusion, complexity, cost and duplication of effort' and the need to maintain publicly available information in 'two quarantined sets—credit reporting and general personal information'.[109]

ALRC's view

54.95 The ALRC no longer considers that the definition of a 'credit reporting business' should be amended, as proposed in DP 72. The proposal alone is not capable of achieving the policy position intended by the OPC—that is, to regulate publicly available personal information collected by a credit reporting agency for credit assessment purposes under Part IIIA (or the new credit reporting regulations) rather than the NPPs (or UPPs).

54.96 The exclusion of the words 'records in which the *only* personal information relating to individuals is publicly available information' (emphasis added) would have limited effect as credit reporting agencies do not often provide publicly available information to credit providers in isolation from other personal information. In any case, the provisions of Part IIIA (and the new credit reporting regulations) apply to the handling of credit information files and credit reports (or credit reporting information in the new regulations), which are permitted to contain only specified categories of personal information.[110]

---

107 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

108 Veda Advantage, *Submission PR 498*, 20 December 2007.

109 Ibid.

110 The OPC noted that the permitted contents of a credit information file would need to be expanded to cover additional categories of publicly available information: Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

54.97 One rationale for the proposal was that it was consistent with the ALRC's proposal that the *Privacy (Credit Reporting Information) Regulations* permit credit reporting information to include publicly available information.[111] As discussed in Chapter 56, the ALRC has concluded that no case has been made for the inclusion of new categories of publicly available information in credit reporting information.

54.98 The definition of 'credit reporting information' (see Recommendation 54–3 above) in the new *Privacy (Credit Reporting Information) Regulations* should continue to ensure that publicly available information maintained by a credit reporting agency is covered by credit reporting regulation only where the information is maintained 'in the course of carrying on a credit reporting business'—that is, consumer credit reporting. As is presently the case under Part IIIA of the *Privacy Act*, a credit reporting agency should be able to conduct other business undertakings, including commercial credit reporting, using publicly available or other personal information that it holds, subject to compliance with the UPPs and other obligations under the *Privacy Act*.

54.99 As noted above, a 'credit reporting agency' is currently defined as a 'corporation' that carries on a credit reporting business.[112] Consistent with the ALRC's overall approach to reform, a credit reporting agency under the new *Privacy (Credit Reporting Information) Regulations* should be defined as any 'agency or organisation'—as those terms are defined in the *Privacy Act*—that engages in a credit reporting business.

54.100 If the small business exemption is not removed from the *Privacy Act* (as recommended in Chapter 39) regulations should be made under s 6E to ensure credit reporting agencies or credit providers that are small business operators are treated as organisations for the purposes of the Act and the *Privacy (Credit Reporting Information) Regulations*.

Credit providers

54.101 In general, credit reporting agencies may disclose personal information contained in credit information files (for example, a credit report) only to those persons who are 'credit providers' as that term is defined in the Act.[113] An entity is a credit provider under s 11B if the entity is, among other things, a

- bank;
- corporation, a substantial part of whose business or undertaking is the provision of loans;

---

111 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–6.
112 *Privacy Act 1988* (Cth) s 11A.
113 These provisions are summarised in more detail in Ch 53.

- corporation that carries on a retail business in the course of which it issues credit cards; or

- corporation that provides loans and is included in a class of corporations determined by the Privacy Commissioner to be credit providers for the purposes of the *Privacy Act*.[114]

54.102 A loan is defined to include a hire-purchase agreement or an agreement for the hiring, leasing or renting of goods or services under which full payment is not made or a full deposit is paid for the return of goods.[115]

Credit provider determinations

54.103 The Privacy Commissioner has made two determinations of general application[116] in relation to the definition of credit provider under s 11B. These determinations were renewed from August 2006 and are effective to 31 August 2011.

54.104 Under the Privacy Commissioner's *Credit Provider Determination No. 2006–4 (Classes of Credit Provider)* (Classes of Credit Provider Determination)—first made in substantially similar form in 1991—corporations are to be regarded as credit providers if they:

- make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least seven days; or

- engage in the hiring, leasing or renting of goods, where no amount, or an amount less than the value of the goods, is paid as deposit for return of the goods, and the relevant arrangement is one of at least seven days duration.[117]

54.105 Under the Privacy Commissioner's *Credit Provider Determination No. 2006–3 (Assignees)* (Assignees Determination)—first made in substantially similar form in 1995—corporations are to be regarded as credit providers for the purposes of the *Privacy Act* if they acquire the rights of a credit provider with respect to the repayment of a loan (whether by assignment, subrogation or other means). A corporation deemed to be a credit provider by virtue of the Assignees Determination is regarded as the credit provider to whom the loan application was submitted, or who provided the loan.[118]

---

114 *Privacy Act 1988* (Cth) s 11B(1)(b)(v)(B).

115 Ibid s 6(1), definition of 'loan'.

116 A third credit provider determination relates to a particular Australian Government agency and is not discussed here: Privacy Commissioner, *Credit Provider Determination No 2006–5 (Indigenous Business Australia)*, 25 October 2006.

117 Privacy Commissioner, *Credit Provider Determination No. 2006–4 (Classes of Credit Providers)*, 21 August 2006.

118 Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006.

Participation in the credit reporting system

54.106 The definition of credit provider raises broad issues about who should be permitted to participate in the credit reporting system; and what standards participants should have to comply with, in relation to credit reporting and more generally.

54.107 There have been suggestions, for example, that credit providers should have to comply with the *Consumer Credit Code* in order to participate in the credit reporting system.[119] The *Consumer Credit Code*, which has been adopted by all state and territory governments, governs many aspects of credit transactions and provides a range of important protections for consumers. These protections include, for example, notice requirements that must be met before a credit provider may begin enforcement proceedings, prescribed periods within which a default may be remedied by the consumer,[120] and the power of a court to reopen an unjust transaction.[121]

54.108 Some organisations, which are recognised as credit providers for the purposes of the credit reporting provisions of the *Privacy Act*, are not required to comply with the *Consumer Credit Code*, which applies to 'credit providers' defined more narrowly.[122] Importantly, the *Consumer Credit Code* 'does not recognise services provided with payment in arrears terms as credit'.[123]

Discussion Paper proposal

54.109 In DP 72, the ALRC proposed that the *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the *Privacy Act* should generally continue to be credit providers for the purposes of the regulations.[124]

54.110 The ALRC also asked whether the new definition of credit provider could be tightened at the margins and, in particular, whether organisations should be regarded as credit providers if they make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least 30 days—as

---

119 Office of the Privacy Commissioner, *Report on the Review of the Credit Provider Determinations (Assignees and Classes of Credit Providers)* (2006), 15.

120 *Consumer Credit Code* ss 80–81.

121 In determining whether a transaction is unjust, the court may have regard to, among other things, whether 'the credit provider knew, or could have ascertained by reasonable inquiry of the debtor at the time, that the debtor could not pay': Ibid s 70(2)(l).

122 Under the *Consumer Credit Code*, a 'credit provider' is defined to mean a person who provides 'credit': Ibid s 3(1), Sch 1. For the purposes of the Code, credit is provided if, under a contract, 'payment of a debt … is deferred' or a person 'incurs a deferred debt to another': *Consumer Credit Code* s 4(1). The *Consumer Credit Code* applies only to the provision of credit where a charge is or may be made for providing the credit: *Consumer Credit Code* s 5(1).

123 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

124 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–7.

compared to seven days, as is currently the case under the Classes of Credit Provider Determination.[125] This would bring the definition into line with common trade terms relating to payment for invoiced goods or services.

54.111 Finally, the ALRC asked whether the definition of 'credit provider' under the NZ Code should be adopted as the definition of 'credit provider' under the new *Privacy (Credit Reporting Information) Regulations*.[126] Under the NZ Code, a credit provider is defined as an entity 'that carries on a business involving the provision of credit to an individual'. The term 'credit' means 'property or services acquired before payment, and money on loan'.[127] This option, in contrast to the preceding suggestion, would loosen the definition of credit provider.

Submissions and consultations

54.112 The proliferation of entities that have access to the credit reporting system—due primarily to the breadth of the definition of credit provider under the Privacy Commissioner's determinations—was highlighted in submissions.[128] The Privacy Commissioner's credit provider determinations have extended access to the credit reporting system 'beyond traditional lenders such as banks to a wide range of retailers and service providers' including, for example, video store operators, and legal services and healthcare providers.[129]

54.113 Some stakeholders maintained that, in reaching these determinations, the Commissioner had failed 'to strike the correct balance' between commercial interests and protecting the privacy of credit reporting information.[130] Legal Aid Queensland observed:

> In 16 years of making determinations in respect of the categories of credit providers who can access credit reporting, the privacy commissioner has facilitated the astronomical expansion of potential entities who can access credit reporting. We note that when the credit reporting provisions of the *Privacy Act* commenced in 1991, there was an expectation that the restrictive nature of the legislation would mean that there would be less than 500 members. Veda Advantage now claim more than 5000 corporate members.[131]

---

125 Ibid, Question 50–1.
126 Ibid, Question 50–2.
127 *Credit Reporting Privacy Code 2004* (NZ) cl 5.
128 For example, Queensland Law Society, *Submission PR 286*, 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007.
129 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.15]. In this context, Tasmanian Collection Service observed that organisations which 'typically provide small value credit' include veterinary surgeons, medical specialists, florists, schools and newsagents: Tasmanian Collection Service, *Submission PR 375*, 5 December 2007.
130 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.
131 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

Telecommunications and utilities

54.114 One focus of concern has been on access to the credit reporting system by telecommunications and utilities companies.[132] Telecommunications and utilities companies use the credit reporting system to assess the credit worthiness of applicants for accounts and to assist in debt collection. These companies also may report overdue payments (defaults). For the purposes of credit reporting regulation, 'credit' advanced by telecommunications companies involves, for example, 'post-paid services'. These are where services are provided without requiring immediate payment by the customer, such as (in the case of Telstra) 'fixed home phone connection and call charges, post-paid mobile call charges and BigPond usage charges for dial-up, ISDN and broadband'.[133]

54.115 Telecommunications and utilities companies are credit providers for the purposes of Part IIIA of the *Privacy Act* by virtue of the Classes of Credit Provider Determination. These companies are not generally bound to comply with the provisions of the *Consumer Credit Code.* A number of stakeholders submitted that compliance with the *Consumer Credit Code* should be a condition of access to the credit reporting system.[134] The Banking and Financial Services Ombudsman (BFSO), for example, submitted that access should not be allowed unless the credit that has been provided is regulated credit, as defined in the *Consumer Credit Code*.[135]

54.116 Some stakeholders suggested that telecommunications companies are inadequately regulated as credit providers.[136] In response, telecommunications and utilities companies emphasised their need for credit reporting information and the fact that credit management in telecommunications is subject to an industry credit management code released by the Australian Communications Industry Forum.[137]

---

132 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007.

133 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

134 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007. The OPC supported the 'alignment' of the definition of 'credit' in the *Privacy Act* with the definition in the *Consumer Credit Code*: Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

135 Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007.

136 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 24.

137 Australian Communications Industry Forum, *Industry Code—Credit Management*, ACIF C541 (2006). The credit management code was registered by the Australian Communications and Media Authority on 13 April 2006 and binds telecommunications carriers and carriage service providers. The code deals with, among other things: the steps undertaken to enable a consumer to gain and maintain access to services (including credit assessment and credit control); the minimum steps (including acceptable minimum timeframes for advising consumers) that a supplier must take before suspending, restricting or

54.117 Optus noted that, without access to credit reporting information, it would be 'forced to undertake more intrusive information collection in order to assess the level of risk of providing that customer with a service'.[138] EnergyAustralia stated that it would be 'unfair to allow one particular class of credit provider access to information that enables them to make judgements about credit worthiness and deny this to another class of credit providers'.[139]

Access to credit reporting information

54.118 While most concern centred on the provisions of the Classes of Credit Provider Determination, discussed above, some stakeholders argued that, in some respects, the definition of credit provider is too restrictive and excludes some businesses that have legitimate claims to have access to credit reporting information.

54.119 The AFC, for example, stated that the definition should be 'broadened to cover any business that supplies goods or services other than on an up-front cash basis' and the definition should not rely on any limit based on a fixed number of days for which payment is deferred.[140]

54.120 There are some classes of organisation that do not meet the current criteria for participation in the credit reporting system but consider that they should be permitted to obtain personal information contained in credit information files. Mercantile agents and others engaged in debt collection, investigation and related activities comprise one such group. Real estate agents and landlords comprise another.[141]

54.121 There are concerns, however, about access to credit reporting by 'non-traditional lenders' on the basis that the information obtained is primarily used in debt collection, rather than risk assessment, and by businesses that are more likely not to have appropriate dispute resolution or data quality processes in place.[142] The Assignees Determination was criticised in this context. National Legal Aid, for example, stated that assignees 'are typically debt collection agencies, which are thus given access to an information resource which was originally intended to exclude them from direct access to credit information files'.[143]

---

disconnecting a consumer's services; the processes that follow disconnection of services, including the collection of debts; and the disclosure of consumer personal information to a third party that may take place as a consequence of credit management action: Australian Communications Industry Forum, *Industry Code—Credit Management*, ACIF C541 (2006), i.

138 Optus, *Submission PR 258*, 16 March 2007.

139 EnergyAustralia, *Submission PR 229*, 9 March 2007.

140 Australian Finance Conference, *Submission PR 294*, 18 May 2007.

141 The NZ Code specifically permits a credit reporter to disclose credit information (where authorised by the individual) to a prospective landlord for the purpose of assessing the credit worthiness of the individual as a tenant: *Credit Reporting Privacy Code 2004* (NZ) r 11(2)(b)(ii).

142 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

143 The assignment or factoring of debts, including debts that are not overdue is, however, a common commercial practice: Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007.

Definition of credit provider

54.122 There was support for the incorporation of a simplified definition of credit provider[144] in the *Privacy (Credit Reporting Information) Regulations*, but stakeholders had different perspectives on the desirable content of such a definition. Industry stakeholders, understandably, favoured a formulation that would maintain access to the credit reporting system for those organisations that currently have access.[145]

54.123 The OPC agreed that the definition should permit those individuals and organisations that are currently credit providers for the purposes of the *Privacy Act* to continue to be credit providers under the new regulations.[146] The Uniform Consumer Credit Code Management Committee specifically supported continued access to credit reporting information by telecommunications providers in order to allow those companies 'to screen out customers'.[147]

54.124 The Cyberspace Law and Policy Centre supported a narrower definition of credit provider than is currently provided under the Act and the Privacy Commissioner's credit provider determinations.

> Given the potential effect on individuals of adverse conclusions being drawn from credit reports, it is essential that access is limited to genuine lenders who can justify the need for credit reporting information. Businesses such as car hire firms and real estate agents, and employers, who seek to use credit reporting information for other purposes, must continue to be denied access, as must merchants accepting credit card payments who do not bear the risk of defaults.[148]

54.125 The Cyberspace Law and Policy Centre suggested that any simplified definition of credit provider 'should not be significantly broader than the current definition' and 'the justification for the classes included by Determination should be revisited'.[149] Other stakeholders also submitted that current credit providers should not

---

144 GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; First Data International, *Submission PR 503*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

145 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

146 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

147 Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007.

148 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

149 Ibid.

necessarily retain access to the credit reporting system[150]—particularly if more comprehensive reporting is to be introduced.[151]

54.126 There was some support for increasing the required deferred payment period to 30 days.[152] It was said that such a reform would be 'likely to capture most of the problematic small credit providers who currently can potentially access credit reporting including video companies, car hire companies and most tradespeople'.[153] The idea was specifically opposed by other stakeholders, on the grounds that organisations with a legitimate need for credit reporting information would be excluded, including telecommunications providers.[154]

54.127 Views were similarly mixed on the appropriateness of the broad definition of credit provider found in the NZ Code. Some industry stakeholders submitted that such a definition would form an appropriate starting point for the definition of credit provider under Australian credit reporting regulation.[155] Others opposed the idea.[156] Legal Aid Queensland, for example, stated:

> Such a definition would provide access to credit reporting to employers, car hire companies, insurers, debt collectors, real estate agents, corner stores (particularly in aboriginal communities where 'bookup' is a significant issue), newsagents (who provide daily deliveries but charge for service, on a periodical basis in arrears), doctors, dentists, lawyers and plumbers leaving very few entities that could not potentially access credit reporting.[157]

54.128 ARCA suggested that the new regulations should define a 'credit provider' as 'an organisation that carries on a business involving the provision of credit to an individual' and 'credit' as 'property or services acquired before payment and money on loan'—the formulation used in the NZ Code.[158] This position was also favoured by other industry stakeholders.[159] Some stakeholders went further. The Australian Credit

---

150 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

151 National Legal Aid, *Submission PR 521*, 21 December 2007.

152 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

153 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

154 Optus, *Submission PR 532*, 21 December 2007; First Data International, *Submission PR 503*, 20 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

155 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

156 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

157 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

158 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

159 Veda Advantage, *Submission PR 498*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007. The AFC favoured a similar broad definition of 'credit provider': Australian Finance Conference, *Submission PR 398*, 7 December 2007.

Forum, for example, suggested that the definition also should include any business that accepts cheques.[160]

54.129 Other stakeholders expressed concerns about an overly broad definition of credit provider, such as that in the NZ Code, whether or not qualified by a deferred payment period. The Consumer Action Law Centre stated:

> Our view is that the number of days allowed for payment is not the key issue, but the amount of risk being taken by the business. For example, allowing 60 days to pay a small account may present little risk, while allowing 5 days to pay for, say, a vehicle that has already been delivered would be a significant risk.[161]

54.130 It was also suggested that the *Privacy (Credit Reporting Information) Regulations* should provide a power for the OPC to determine that an organisation is, or is not, a credit provider for the purpose of the Act and regulations—that is, a power similar to the existing OPC power under s 11B(1)(b)(v)(B).[162] The OPC submitted that:

> The Privacy Commissioner should retain the power to deem businesses as credit providers by making determinations. Businesses that are currently deemed to be credit providers by determination should not be incorporated into the statutory definition of credit provider but be covered by a determination.[163]

54.131 The OPC provided a number of detailed comments on the definition of credit provider and related matters.[164] The OPC submitted that the related definition of 'loan' should be amended so that, where a 'loan' concerns the hire, lease, or rental of goods, a payment is defined as either a deposit or a payment in advance and the value of the goods is assessed by an objective standard.[165] The OPC also suggested that the meaning of 'substantial', which forms part of the definition of 'credit provider' in s 11B(1)(b)(iii) of the *Privacy Act*, could be improved; and state and territory government agencies that make loans to individuals should have the same opportunity as Australian government agencies to apply for a credit provider determination.[166]

ALRC's view

54.132 The ALRC is not convinced that there is a sufficiently compelling case to tighten the definition of credit provider for the purpose of new credit reporting

---

160 Australian Credit Forum, *Submission PR 492*, 19 December 2007.

161 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

162 Veda Advantage, *Submission PR 498*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

163 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

164 Ibid.

165 The existing definition of 'loan' in *Privacy Act 1988* (Cth) s 6(1) excludes a contract for hire, lease or rent of goods under which an amount greater than or equal to the value of the goods is paid as deposit for the return of the goods.

166 See Ibid s 11B(1)(d).

regulation. The credit provider determinations have been in place since 1991 and commercial practices have developed in reliance on continued access to credit reporting information.

54.133 The determinations were reviewed and renewed without substantive amendment by the OPC in 2006. The OPC concluded that, while there were recurring issues that required attention, these issues had not prevented the Classes of Credit Provider Determination from operating satisfactorily.[167] The OPC undertook to develop information sheets and education strategies targeted at businesses covered by the Classes of Credit Provider Determination and those operating in the telecommunications sector; and to consider, as resources became available, the development of a credit reporting audit program focusing on non-traditional credit providers.[168]

54.134 Opponents of access by credit providers covered by the credit provider determinations did not deny that some of these businesses have an operational need for access to credit reporting information to assess the credit worthiness of potential customers. Objections to such access were based in large part on the use of default listing as a debt collection tool and on the quality of data reported by these credit providers. Even some critics of the existing definition of a credit provider accept, however, that there are difficulties in developing viable alternatives that do not exclude organisations with a legitimate need for credit reporting information.

54.135 Many of the concerns about the breadth of the definition of credit provider may be addressed effectively by the ALRC's recommendations intended to improve credit reporting data quality (see Chapter 58) and complaint-handling procedures (Chapter 59). In particular, the ALRC recommends that the *Privacy (Credit Reporting Information) Regulations* should provide that credit providers may only list overdue payment information where the credit provider is a member of an external dispute resolution (EDR) scheme approved by the OPC. This recommendation is aimed at improving complaint-handling processes, but may have the secondary effect of removing 'fringe' players from the credit reporting system who are unwilling to join an EDR scheme.

54.136 As proposed in DP 72, the ALRC recommends that the *Privacy (Credit Reporting Information) Regulations* include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the *Privacy Act* should generally continue to be credit providers for the purposes of the new regulations. In the ALRC's view, no compelling

---

167 Office of the Privacy Commissioner, *Report on the Review of the Credit Provider Determinations (Assignees and Classes of Credit Providers)* (2006), 20.

168 Ibid, 22. The OPC also concluded that the Assignees Determination was operating satisfactorily and recommended that education programs should be developed and audit programs considered: Office of the Privacy Commissioner, *Report on the Review of the Credit Provider Determinations (Assignees and Classes of Credit Providers)* (2006), 20, 22.

case has been made out for organisations to be regarded as credit providers if they provide goods or services on terms that allow the deferral of payment for at least 30 days, as discussed in DP 72.[169]

54.137 Beyond this, the ALRC does not have a firm view on exactly how the definition should be drafted. As discussed above, a range of issues concerning the drafting of the definition were raised in DP 72, and put forward in submissions. The definition will inevitably be broad, to avoid arbitrary distinctions between organisations that face credit risks. The finer detail of the drafting is, however, best left to the Australian Government to resolve, with the assistance of the Office of Parliamentary Counsel.

Recommendation 54–4 The new *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of 'credit provider' under which those agencies and organisations that are currently credit providers for the purposes of the *Privacy Act* (whether by operation of s 11B or pursuant to determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.

Application to foreign credit providers

54.138 There has been some concern about the: (a) listing on credit information files of information about foreign credit; and (b) disclosure of credit reports to foreign credit providers.[170] For example, as some credit reporting agencies operate in both New Zealand and Australia, individuals applying for credit in Australia may have default listings relating to loans from New Zealand credit providers.

54.139 Under the *Privacy Act*, a credit provider is defined to include a corporation if a substantial part of its business or undertaking is the provision of loans.[171] In turn, a corporation includes a foreign corporation within the meaning of s 51(xx) of the *Australian Constitution*.[172]

54.140 The provisions of s 5B of the *Privacy Act* dealing with its application to acts and practices outside Australia do not apply to the credit reporting provisions.[173] In particular, the Privacy Commissioner is not empowered to take action outside Australia

169 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 50–1.
170 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.163].
171 See *Privacy Act 1988* (Cth) s 11B.
172 Ibid s 6(1) definitions of 'corporation' and 'foreign corporation'.
173 Ibid s 5B(1).

to investigate credit reporting complaints.[174] The OPC faces difficulties in investigating complaints about information from foreign credit providers, given limitations on the extraterritorial operation of Part IIIA. In response to these concerns, Veda Advantage does not include information about foreign loans in its credit reports.

54.141 More generally, there may be no means to ensure that a foreign credit provider complies with any of the obligations of credit providers under Part IIIA—for example, in relation to notifying individuals that information may be disclosed to a credit reporting agency.

54.142 The OPC, based on the statutory construction of Part IIIA, has taken the view that

> the listing of overseas incurred loans (and any information relating to those loans) on an individual's credit information file and the disclosure of personal information in credit information files … to a party overseas is not permitted by Part IIIA.[175]

Discussion Paper proposals

54.143 In DP 72, the ALRC proposed that the:

- new *Privacy (Credit Reporting Information) Regulations* should exclude the reporting of personal information about foreign credit and foreign credit providers, and the disclosure of credit reporting information to foreign credit providers;[176] and

- Australian Government should consider including credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).[177]

54.144 With some qualifications, mostly involving the desirability of harmonisation of trans-Tasman rules, stakeholders supported excluding foreign credit providers from access to the Australian consumer credit reporting system.[178]

---

174 Ibid s 5B(4).

175 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

176 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–8.

177 Ibid, Proposal 50–9.

178 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. The Law Society of New South Wales, in contrast, stated that foreign credit providers should be encouraged to make reports to Australian credit reporting agencies: Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

54.145 The OPC expressed the view that practical and jurisdictional difficulties dictate that foreign credit providers and foreign loans should continue to be excluded from regulation under the *Privacy Act*. The OPC supported the express exclusion in the new *Privacy (Credit Reporting Information) Regulations* of:

> (a) information about credit incurred in foreign countries;
>
> (b) access to the Australian credit reporting system by credit providers based overseas; and
>
> (c) the disclosure of credit reporting information to credit providers or credit reporting agencies based overseas.[179]

54.146 Other stakeholders also expressed concern that about the privacy risks and enforcement difficulties involved with access by foreign credit providers.[180] Some supported access by foreign credit providers[181] or considered that, if foreign credit providers can demonstrate compliance with data security and complaint-handling procedures, they should be permitted to access credit reporting information in Australia.[182]

54.147 ARCA and a number of other industry stakeholders agreed that, for the time being, foreign credit providers should be excluded, but that this position should be subject to review in light of the potential future benefit of extending the credit reporting system.[183] New Zealand was seen as a special case,[184] given

> the geographic location of NZ to Australia, the frequency of migration of residents between the two countries, and the Australian Government's commitment to greater harmonisation between Australia and NZ's laws particularly in the banking and consumer protection regulatory framework … evidenced in cross-border company recognition and insolvency provisions.[185]

---

179 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

180 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007.

181 Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007.

182 Queensland Law Society, *Submission PR 286*, 20 April 2007.

183 GE Money Australia, *Submission PR 537*, 21 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

184 For example, Australian Credit Forum, *Submission PR 492*, 19 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

185 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

54.148 The desirability of trans-Tasman flows of credit reporting information was emphasised.[186] Veda Advantage stated that it sought 'urgent measures' to 'permit trans-Tasman access to credit reporting for business and consumers'.[187]

54.149 The AFC and the Australian Credit Forum[188] considered that, at the very least, a New Zealand credit provider should be able to obtain a copy of an Australian citizen's credit report from an Australian credit reporting agency while that individual is resident in New Zealand—as 'to prevent such access may operate to disadvantage the customer in relation to their access to appropriate and effectively-priced credit while in NZ'.[189]

54.150 Stakeholders agreed that, if greater consistency between Australian and New Zealand credit reporting regulation can be achieved, credit reporting information from both countries should be available from Australian credit reporting agencies. The ALRC's proposal to identify credit reporting regulation as an issue for the business law coordination agenda met with broad approval.[190] Concerns were expressed, however, that any harmonisation process should not adopt the NZ Code as the template for future legislation or lead to less stringent regulation of credit reporting.[191]

ALRC's view

54.151 Issues concerning the participation of foreign credit providers are linked to the regulation of cross-border data flows, which is discussed in Chapter 31. The draft 'Cross-border Data Flow' principle is designed to regulate the transfer of Australian credit reporting information overseas, but has nothing to say about inward data flows—for example, a default report from a foreign credit provider that is transferred to an Australian credit reporting agency.

54.152 Such a provision could be built into the new *Privacy (Credit Reporting Information) Regulations* so that, for example, foreign credit providers may report credit reporting information if they are subject to a law, binding scheme or contract

---

186 Australian Finance Conference, *Submission PR 294*, 18 May 2007; Veda Advantage, *Submission PR 272*, 29 March 2007; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007; Australian Institute of Credit Management, *Submission PR 224*, 9 March 2007.

187 Veda Advantage, *Submission PR 272*, 29 March 2007.

188 Australian Credit Forum, *Submission PR 492*, 19 December 2007.

189 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

190 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

191 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

which effectively upholds principles for fair handling of credit reporting information that are substantially similar to those in the new regulations.[192]

54.153 As discussed above, however, the primary concern about the reporting of personal information by overseas credit providers relates to the availability of effective enforcement and complaint handling. On this basis, the ALRC recommends that the *Privacy (Credit Reporting Information) Regulations* should generally exclude the reporting of personal information about foreign credit and foreign credit providers; and the disclosure of credit reporting information to foreign credit providers.

54.154 There should, however, be some mechanism by which credit reporting across jurisdictional boundaries may be permitted—in particular, between Australia and New Zealand. The Australian and New Zealand banking and financial services markets are highly integrated and many credit providers (and both major credit reporting agencies) operate on both sides of the Tasman. The New Zealand Privacy Commissioner observed, in this context, that 'consumer credit reporting is an activity in which the same major companies dominate business on both sides of the Tasman' and urged the ALRC to consider 'the trans-Tasman angle'.[193]

54.155 There are important benefits in promoting harmonisation in the area of credit reporting, and harmonisation may ultimately permit integration of regulatory systems. Starting from their similar legal and commercial backgrounds, New Zealand and Australia have already achieved a significant degree of coordination and cooperation in a number of areas of business law (including in fair trading and other consumer protection law).

54.156 The countries are committed to further development of business law coordination under the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).[194] Recent progress in this regard has involved cross-border company recognition, cross-border insolvency provisions, mutual bans on disqualified company directors and information sharing between trans-Tasman competition and consumer regulators.[195] Coordination of credit reporting regulation would be a subject consistent with this overall agenda.

54.157 Trans-Tasman transfer of credit reporting information, however, need not necessarily await the outcome of a business law coordination process. In the ALRC's

---

192 See Ch 31.

193 New Zealand Privacy Commissioner, *Submission PR 128*, 17 January 2007.

194 *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000) Department of Foreign Affairs and Trade <www.dfat.gov.au/geo/new_zealand/anz_cer/memorandum_of_understanding_business_law.html> at 5 May 2008.

195 P Costello (Australian Government Treasurer) and M Cullen (New Zealand Minister for Finance), 'Bilateral Progresses Single Economic Market Agenda' (Press Release, 29 January 2007).

view, the new *Privacy (Credit Reporting Information) Regulations* should empower the Privacy Commissioner to approve the reporting of personal information about foreign credit; and the disclosure of credit reporting information to foreign credit providers, in defined circumstances.

54.158 The criteria for approval should include the availability of effective enforcement and complaint handling in the other jurisdiction. In this context, the OPC and the Office of the New Zealand Privacy Commissioner are well placed to build upon existing relationships, reflected in their 2006 Memorandum of Understanding.[196] This memorandum, among other things, records the intention of the respective offices to 'cooperate in relation to complaints or investigations that may affect the other participant or have a cross-border element'; and 'explore the usefulness of developing more detailed protocols for handling complaints that may affect the other participant or that have a cross-border element'.[197]

54.159 Given the existing similarities between credit reporting regulation in Australia and New Zealand—and links between New Zealand and Australian credit providers, credit reporting agencies, and privacy regulators—appropriate mechanisms may be able to be developed to allow trans-Tasman transfer of credit reporting information to be approved. There is, for example, nothing to prevent a New Zealand credit provider agreeing to be bound by the terms of an Australian-based EDR scheme, as a condition of access to Australian credit reporting information.

Recommendation 54–5 The new *Privacy (Credit Reporting Information) Regulations* should, subject to Recommendation 54–7, exclude the reporting of personal information about foreign credit and the disclosure of credit reporting information to foreign credit providers.

Recommendation 54–6 The Australian Government should include credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).

196 Office of the Australian Privacy Commissioner and Office of the New Zealand Privacy Commissioner, *Memorandum of Understanding Between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner*, 4 September 2006.

197 Ibid, [8.1], [8.4].

Recommendation 54–7 The new *Privacy (Credit Reporting Information) Regulations* should empower the Privacy Commissioner to approve the reporting of personal information about foreign credit, and the disclosure of credit reporting information to foreign credit providers, in defined circumstances. The regulations should set out criteria for approval, including the availability of effective enforcement and complaint handling in the foreign jurisdiction.

Consumer and commercial credit

54.160 Part IIIA distinguishes between consumer and commercial credit reporting. Part IIIA regulates consumer credit reporting activities, but does not cover personal information about commercial loans (that is, loans not intended to be used wholly or primarily for domestic, family or household purposes).[198] The handling of personal information relating to commercial loans (referred to below as 'commercial credit reporting information') is regulated primarily by the NPPs.

54.161 Part IIIA, however, touches on some aspects of commercial credit reporting. For example, s 18E(1)(b) permits credit reports to contain information about commercial credit and there are complex provisions to the effect that information about consumer credit can be used in commercial credit transactions, and vice versa, provided that agreement of the individual concerned is obtained.[199] Further, the fact that an individual is the guarantor of a commercial loan is currently permitted content of a credit information file.[200]

54.162 The ALRC asked whether the distinction in the credit reporting provisions of the *Privacy Act* between consumer and commercial credit is necessary or whether personal information about consumer and commercial credit should be regulated by the same statutory provisions.[201]

198 *Privacy Act 1988* (Cth) s 6(1) definition of 'credit'.

199 Ibid ss 18K(1)(b), 18L(4).

200 Under s 18E(1)(b)(iv), permitted content includes information in connection with an individual having offered to act as a guarantor in respect of a 'loan'. A 'loan', unlike 'credit', is not defined as being for 'domestic, family or household' purposes: Ibid s 6(1).

201 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–25.

54.163 Most stakeholders who addressed the issue favoured retaining the distinction between consumer and commercial credit reporting.[202] This view was influenced, at least in part, by the fact that the *Consumer Credit Code* makes a similar distinction between credit 'provided or intended to be provided wholly or predominantly for personal, domestic or household purposes', which is regulated by the Code, and other credit, which is not.[203]

54.164 On the other hand, the OPC noted that credit reporting agencies currently make an individual's commercial credit transactions available to credit providers to assess an individual's credit eligibility and that some provisions of Part IIIA already regulate aspects of commercial credit granted to individuals. This 'fragmented approach adds to the complexity of the provisions'.[204]

Discussion Paper proposal

54.165 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should apply to personal information relating to credit advanced to an individual for any purpose and should not be limited to 'domestic, family or household' purposes, as is currently the case under the definition of 'credit' in the *Privacy Act*.[205]

54.166 In making this proposal, the ALRC noted that the current distinction between consumer and commercial credit may create needless complexity and appears inconsistent with the general approach of the *Privacy Act*. The Act does not distinguish in any other respect between personal information about an individual's personal and commercial activities. The distinction is not made in the NZ Code, which simply covers personal information that is credit information.

54.167 This proposal was opposed strongly by industry stakeholders.[206] ARCA and others[207] submitted that there are good reasons to continue to exclude commercial credit reporting information from credit reporting privacy regulation. First, commercial credit reporting information is adequately protected as personal information by privacy

---

202 Australian Finance Conference, *Submission PR 294*, 18 May 2007; Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007; EnergyAustralia, *Submission PR 229*, 9 March 2007; Australian Institute of Credit Management, *Submission PR 224*, 9 March 2007. Some of these comments were premised on a misapprehension that regulation of credit reporting in respect of corporate entities was being contemplated.

203 *Consumer Credit Code* s 6(1)(b).

204 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

205 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–10.

206 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

207 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

principles—where it is 'about' an individual.[208] Secondly, if commercial credit reporting information (for example, about sole traders and unincorporated partners) were covered by the new *Privacy (Credit Reporting Information) Regulations*, then commercial credit reporting would be subject to new requirements, beyond those imposed by the UPPs, in relation to the collection, use and disclosure of information and complaint handling. The undesirable consequences of this were said to include:

> (i) Significant additional compliance costs for the commercial credit reporting sector (access and correction; re-tooled business processes)
>
> (ii) Significant additional compliance costs for commercial credit providers (EDR, additional statutory notice requirements)
>
> (iii) Different treatment of commercial debtors who are superficially similar: a sole trader's record would have additional protection; if the same or similar business were incorporated as an association or a company, even if it were smaller, it would not have the protection
>
> (iv) Departure from the general consumer protection principle (FSR and UCCC) that people in business have less need of higher standards of protection (including disclosure)
>
> (v) The consumer credit market is very different from the trade and commercial credit markets, and the primary purpose is likely to unreasonably constrain credit reporting in commercial contexts.[209]

54.168 Other industry stakeholders made similar points. The National Australia Bank stated that the ALRC's proposal 'has the potential to extend requirements into the small business segment which could make the regulation unworkable'.[210] Telstra submitted that the proposal

> appears out of step with the 'consumer protection' purpose of the provisions dealing specifically with consumer credit information. Unlike consumer credit, an individual's commercial credit activities do not receive the protection of the *Consumer Credit Code*. Given their nature, these commercial activities are generally subject to less onerous legislation on credit providers.[211]

54.169 The OPC's position remained that the new *Privacy (Credit Reporting Information) Regulations* should apply to personal information relating to credit sought or obtained by an individual for any purpose and not limited to 'domestic, family or

---

208 See, *Privacy Act 1988* (Cth) s 6(1) definition of 'personal information'.

209 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

210 National Australia Bank, *Submission PR 408*, 7 December 2007.

211 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. Other stakeholders also focused on the desirability of maintaining a distinction between commercial and consumer credit, consistent with the *Consumer Credit Code*: Australian Credit Forum, *Submission PR 492*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007.

household' purposes as is currently the case under the definition of 'credit' in the *Privacy Act*.[212]

54.170 A number of other stakeholders agreed.[213] In relation to the consistency of credit reporting regulation and the *Consumer Credit Code*, Legal Aid Queensland noted that the Code is presumed to apply unless the borrower has signed a 'business purposes declaration':

> This has resulted in many small lenders requiring all borrowers to sign a business purposes declaration and only lending for 'commercial purposes' to avoid the application of the legislation. This has resulted in some very unconscionable loans and unfair lending and enforcement practices. In our view to discourage lenders from avoiding the application of the *Privacy Act*, credit reporting ought to be regulated by reference to whether the person borrowing the funds is an individual or a business not the 'disclosed use of the credit' … If the definition is not broad enough to encompass loans to individuals for commercial purposes it may provide an incentive for some credit providers to list defaults as commercial in nature to avoid the requirement to belong to an EDR scheme.[214]

ALRC's view

54.171 On one view, where credit-related personal information is maintained by a credit reporting agency and is, for example, inaccurate or misleading, an individual should have the same rights of recourse regardless of whether the credit advanced was for a consumer or commercial purpose.

54.172 The fact that the *Consumer Credit Code* makes a distinction between consumer and commercial credit does not dictate the retention of a similar distinction in credit reporting regulation. While credit reporting regulation under the *Privacy Act* can be seen as serving a consumer protection purpose, the focus of the Act is on the protection of the information privacy of individuals—regardless of the precise content of personal information.[215]

54.173 The coverage of the regimes already diverges significantly—notably, in relation to which organisations constitute credit providers (discussed above). In any case, the distinction contained in the Code is breaking down. The Uniform Consumer Credit Code Management Committee observed:

---

212 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

213 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

214 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

215 Credit-related information concerning an individual, however, may not constitute personal information if it is, for example, not 'about' an individual but about a company (of which the individual happens to be a director): See, eg, *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

> The forthcoming national finance broker laws … includes protection for both consumers and small business, while it is probably only a matter of time before the Code itself will extend to cover consumer investment and small business credit.[216]

54.174 There is strong opposition from the credit reporting industry and industry stakeholders to an extension of the coverage of credit reporting regulation, especially in view of the possible additional compliance costs. There are justifiable concerns that the provisions of the new *Privacy (Credit Reporting Information) Regulations* may not be appropriate for commercial credit reporting.

54.175 The restrictions on the permitted content of credit reporting information is an example of one such concern. Part IIIA of the Act sets out an exhaustive list of the categories of personal information that may be included in credit information files; a credit reporting agency must not disclose personal information that does not fall within the permitted categories.[217] A similar approach is recommended, with some changes, in the new *Privacy (Credit Reporting Information) Regulations*. It is questionable whether this approach is suitable in the context of commercial lending. The collection and disclosure of a broader set of personal information may be justifiable, with the consent of the individual concerned.

54.176 In any case, commercial credit reporting information receives significant protection under the NPPs, and would continue to do so under the model UPPs. In this context, while the *Privacy Act* extends additional privacy protection to credit reporting information, the regime also authorises some information-handling practices that would not be permitted under the NPPs without the consent of the individual concerned.[218] Bringing commercial credit reporting information into the regime would loosen some aspects of privacy protection, while strengthening others. For example, the credit reporting provisions operate to authorise some secondary use and disclosure of personal information that would not be permitted without consent under the NPPs.[219] Conversely, the credit reporting provisions provide for the deletion of information after the end of maximum permissible periods, whereas the NPPs only oblige organisations to take reasonable steps to ensure that personal information is 'up-to-date'.[220]

---

216 Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007, referring to the *Finance Broking Bill 2007* (Cth).

217 *Privacy Act 1988* (Cth) s 18E(1).

218 For example, s 18N expressly authorises the disclosure by credit providers of personal information to a credit reporting agency; a mortgage insurer; and the assignee of a debt to the credit provider. Under NPP 2.1, such disclosure may require the consent of the individual concerned, depending primarily on whether the specific circumstances authorised by Part IIIA are related secondary purposes within the reasonable expectations of the individual: see also Ch 57.

219 For example, credit reports may be used by mortgage insurers and those considering entering securitisation arrangements, without the individual's consent: *Privacy Act 1988* (Cth) s 18K(1)(ab), (ac), and (d), as compared to NPP 2.1.

220 Ibid s 18F, as compared to NPP 3.

54.177 On balance, the ALRC does not recommend any change to the coverage of credit reporting regulation in relation to commercial credit reporting. The new *Privacy (Credit Reporting Information) Regulations* should apply to personal information relating to credit intended to be used wholly or primarily for 'domestic, family or household' purposes, as provided by the current definition of 'credit' in the *Privacy Act*.

Review of the regulations

54.178 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should be reviewed after five years of operation.[221] The ALRC considered that a requirement to review the regulations was desirable, among other reasons, to assess the impact of more comprehensive credit reporting on privacy and the credit market;[222] and to consider whether further regulation is required to ensure the data quality of credit reporting information.[223]

54.179 A review requirement was supported in submissions[224]—although many stakeholders considered that a review after three years of operation (or even sooner) would be preferable.[225] Galexia submitted:

> The ALRC has proposed that the credit reporting regulatory arrangements should be reviewed after 5 years. In an environment where there are significant concerns about complaints handling processes and culture this review will need to be brought forward. [Galexia] proposes bringing the review forward from 5 years to 3 years.[226]

54.180 The OPC also suggested that consideration should be given at the time of introduction of the *Privacy (Credit Reporting Information) Regulations* to 'appropriate performance criteria and mechanisms for assisting in the review process'. In this

---

221 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 51–3.

222 Ibid, Proposal 51–3. More comprehensive credit reporting is discussed in Ch 55.

223 Ibid, Proposal 54–6. Data quality of credit reporting information is discussed in Ch 58.

224 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Australian Credit Forum, *Submission PR 492*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; MGIC Australia, *Submission PR 479*, 17 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Galexia Pty Ltd, *Submission PR 465*, 13 December 2007; Citibank Pty Ltd, *Submission PR 428*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

225 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Galexia Pty Ltd, *Submission PR 465*, 13 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

226 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.

context, the OPC noted that it 'is not qualified to provide expert opinion on the broader economic and social impact that comprehensive credit reporting may have in Australia'.[227] The OPC submitted:

> Given the proposed focus of the review on the impact of more comprehensive credit reporting on credit markets, and potentially other questions of broader economic and social impact, the Office suggests that the ALRC consider what other appropriate agencies could contribute to or conduct the review process. For example, the Office suggests that a review could be conducted by the Productivity Commission or via a tripartite agreement between the credit reporting agencies, the Office and an independent auditor.[228]

54.181 While other aspects of credit reporting regulation will be important, including problems concerning compliance with the data quality and dispute resolution obligations, the operation of more comprehensive credit reporting can be expected to be a major focus of the review. The ALRC notes that, if the ALRC's recommendations are implemented, it will be some time before the effects of more comprehensive credit reporting can be evaluated. Notably, the model recommended by the ALRC would permit credit reporting agencies to collect an individual's two-year repayment performance history.[229] It will take up to two years at least, therefore, before the system is operating to its full extent. Review of the regulations after five years of operation is appropriate.

Recommendation 54–8 The Australian Government should, in five years from the commencement of the new *Privacy (Credit Reporting Information) Regulations*, initiate a review of the regulations.

Credit reporting code

54.182 In DP 72, the ALRC noted that some matters raised in the Inquiry are not addressed most appropriately through legislation. For example, while credit providers generally support the principle of reciprocity in credit reporting, and obligations to report information consistently, arguably, credit providers themselves and their industry associations should take responsibility for such matters—within the framework provided by legislation.

54.183 The ALRC proposed that credit reporting agencies and credit providers should develop, in consultation with consumer groups and regulators, including the OPC, an

227 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
228 Ibid.
229 See Ch 55, Rec 55–2.

industry code dealing with operational matters such as default reporting obligations and protocols and procedures for the auditing of credit reporting information.[230]

54.184 Stakeholders generally accepted that, in addition to the new *Privacy (Credit Reporting Information) Regulations*, some form of credit reporting code would be desirable.[231] There was less consensus on which specific obligations should be located in the regulations and the code respectively; and on the legal nature of the code.

Content of the code

54.185 Veda Advantage commented that, for a three-tiered regulatory structure to be effective, the regulations should be drafted to be 'inclusive and brief', with detail left to a binding code.

> Many credit reporting operational issues are highly detailed and context specific. It is appropriate that these be contained in an industry code that provides for the ability to update and revise the required provisions as operational issues continue to change.[232]

54.186 The advantages of a code in providing flexibility was emphasised by industry stakeholders.[233] Dun and Bradstreet, for example, stated that the code would 'provide flexibility within a closely governed framework to ensure credit reporting standards and obligations keep pace with industry changes and consumer demands'.[234]

54.187 Galexia put forward broad criteria on which to determine whether specific obligations should be located in the regulations or code. For example, Galexia suggested that matters to be included in regulations should be restricted to those that relate to 'fundamental privacy rights, rather than minor consumer concerns or basic operational matters'. The code, on the other hand, should deal with matters that require significant flexibility, relate to minor consumer or basic operational concerns, or deal with 'industry branding or cooperation'.[235]

---

230 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–11.

231 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Galexia Pty Ltd, *Submission PR 465*, 13 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

232 Veda Advantage, *Submission PR 498*, 20 December 2007.

233 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. Legal Aid Queensland also referred to the advantage of a code in terms of flexibility in adapting to changing credit markets: Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

234 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007.

235 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007. Galexia's position was supported by the Australian Privacy Foundation and the Consumer Law Action Centre: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

54.188 Telecommunications companies had reservations about the desirability of a new credit reporting code.[236] AAPT suggested that, for the telecommunications industry, it may be preferable to augment the existing credit management code.[237] Optus expressed concern about how the proposed code would interact with existing industry codes that deal with the same or similar matters.[238] Telstra highlighted the need to avoid duplication of obligations.[239]

54.189 Other stakeholders stated that privacy protection should not be downgraded by locating obligations currently contained in the *Privacy Act* in an industry code, rather than in legislation.[240] The BFSO, for example, stated that in developing the code it will be important to ensure that

> any matters that are currently the subject of mandatory requirements in Part IIIA or the *Credit Reporting Code of Conduct* remain obligatory (whether by inclusion in the regulations or ensuring that the new code is mandatory and enforceable) ...[241]

54.190 Similarly, the Australian Privacy Foundation supported an industry code, but expressed concern about the meaning of 'operational matters'. The Foundation stated that it 'would see some matters that industry regards as "operational" as more fundamental and would want some of these in Regulations or binding Code/Rules'.[242] The Cyberspace Law and Policy Centre stated that it supported the concept of some detailed operational matters being left to a code but submitted that the ALRC should 'more clearly explain its proposed hierarchy of regulation, and ensure that it recommends placement of specific obligations in the different levels to reflect its conclusions about how "binding" those obligations should be'.[243]

54.191 Throughout the course of the Inquiry, ARCA has been developing a draft code. This code is intended to bind its member organisations in relation to their participation in the credit reporting system. In its submission, ARCA presented detailed proposals on the content of a future code, which it summarised as follows:

> the structure of the code of conduct … is recommended to be in two layers so as to manage in the first layer, policy and compliance and in the second layer operational and procedural matters. The prime rationale for the third tier is to facilitate, under appropriate governance, continuous review and improvement but without the burdens to development and implementation that would apply under regulation. ARCA

---

236 Optus, *Submission PR 532*, 21 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

237 AAPT Ltd, *Submission PR 338*, 7 November 2007. Referring to Australian Communications Industry Forum, *Industry Code—Credit Management*, ACIF C541 (2006).

238 Optus, *Submission PR 532*, 21 December 2007.

239 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

240 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

241 Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007.

242 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

243 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

> recognises that the structure is one that would need to be developed over time with input from stakeholders.[244]

Legal status

54.192 In submissions, stakeholders made a number of comments about the desirable legal status of the proposed code. ARCA proposed that a code of conduct for credit reporting should be developed by industry and then become an approved privacy code under Part IIIAA of the *Privacy Act*, or similar new statutory provision.[245]

54.193 ARCA has also identified a need for the code, or aspects of the code, to be authorised by the ACCC under the *Trade Practices Act 1974* (Cth). It raises potential competition issues, notably in relation to sanctions for non-compliance such as suspension or exclusion from the credit reporting system. ARCA has advised that it is currently pursuing ACCC authorisation for a code of conduct dealing with data standards, and containing sanctions for non-compliance.[246]

54.194 Other industry stakeholders agreed with the ARCA approach.[247] Veda Advantage, for example, submitted that the code of conduct should be:

- Binding on all credit reporting industry participants
- Made by the industry under the *Privacy Act*
- Authorised by the ACCC to ensure that contractual provisions making the Code binding on subscribers of CRAs are lawful.[248]

54.195 Legal Aid Queensland supported a code approved by the Privacy Commissioner and subject to disallowance by Parliament.[249] The OPC referred to its support for 'a voluntary industry code' dealing with operational matters.[250] The Cyberspace Law and Policy Centre noted what it identified as 'considerable uncertainty about the framework proposed by the ALRC—in particular the role of Codes and whether they would be mandatory and/or binding and enforceable'. The Centre favoured the imposition of binding and enforceable subscriber agreements and submitted that the new *Privacy (Credit Reporting Information) Regulations* should require credit reporting agencies to have a complying subscriber agreement in place before disclosing any credit information to a credit provider.[251]

---

244 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.
245 Ibid. See also Rec 48–1.
246 Ibid.
247 Veda Advantage, *Submission PR 498*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.
248 Veda Advantage, *Submission PR 498*, 20 December 2007.
249 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.
250 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
251 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

54.196 An important issue for industry is that, because a credit reporting industry code or agreement is likely to raise competition law issues, it may require authorisation by the ACCC to avoid breaching the *Trade Practices Act*. Galexia noted that

> Authorisation by the ACCC is subject to a very limited test and it is important to clarify that authorisation does not equate with 'approval'. Indeed, the test is simply whether or not the public benefit outweighs any potential lessening of competition that results from the Code.[252]

ALRC's view

54.197 The ALRC recommends that credit reporting agencies and credit providers develop a credit reporting code providing detailed guidance within the framework provided by the *Privacy (Credit Reporting Information) Regulations.* In other chapters, the ALRC makes specific recommendations concerning the desirable content of the code. For example:

- In Chapter 55, the ALRC recommends that the credit reporting code should mandate procedures for the reporting of repayment performance history, within the parameters prescribed by the new regulations (see Recommendation 55–4).

- In Chapter 58, the ALRC recommends that the credit reporting code should promote data quality by mandating procedures to ensure consistency and accuracy in the reporting of overdue payments and other personal information by credit providers (see Recommendation 58–3).

54.198 There may be other matters that should be included. It may be appropriate, for example, for the code to deal with operational matters relevant to dispute resolution (see Chapter 59). Ultimately, however, the content of the code should be determined by the credit reporting industry, in consultation with consumer groups and regulators, including the OPC.

54.199 Consistently with the ALRC's recommendations on codes, the credit reporting code would 'fill in the gaps' between the outcome set by a privacy principle—or, in this case, the new *Privacy (Credit Reporting Information) Regulations*—and the application of, or compliance with, that principle or regulation. In recommending the development of a credit reporting code, the ALRC leaves open the question of the code's precise legal status and governance structure. Again, these are matters for the industry to resolve.

---

252 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007, referring to *Trade Practices Act 1974* (Cth) pt VII, s 90.

54.200 One option would be for the credit reporting code to become an approved code under Part IIIAA of the *Privacy Act*. As discussed in Chapter 48, the ALRC's recommendations for reform of the *Privacy Act* retain the ability of organisations and industries to flesh out the requirements of the privacy principles in privacy codes approved by the Privacy Commissioner under Part IIIAA. The ALRC recommends that the code provisions be changed so that: a code applies in addition to the UPPs (or regulations) and does not replace them; and the primary purpose of a code is to prescribe how a principle or regulation is to be applied or complied with.[253] Privacy codes, under the current provisions and the ALRC's recommended changes, cannot derogate from the principles, unlike regulations and other subordinate legislation.

54.201 A credit reporting code developed by industry or aspects of such a code, could also, under the ALRC's recommended reforms, become incorporated into the *Privacy (Credit Reporting Information) Regulations*, or as a new regulation. Such a regulation could contain provisions that derogate from the privacy principles.

54.202 While it may be desirable, at some future time, for a credit reporting code to be approved under Part IIIAA of the *Privacy Act* or promulgated under the regulations, reform of the credit reporting provisions should not await the development of an approved code. Pending approval under the *Privacy Act*, the code could operate as an industry code, be adopted voluntarily by participants in the credit reporting system, or made enforceable by contract as part of subscription agreements with credit reporting agencies.

54.203 The important point is that the new *Privacy (Credit Reporting Information) Regulations* should be promulgated at the same time that Part IIIA of the Act is repealed. The regulations, in accordance with the recommendations made in this Report, should be capable of providing adequate privacy protection for credit reporting information in the absence of any code. That is, while a code may be desirable, the content of the code should not be essential to the adequate regulation of privacy in credit reporting.

Recommendation 54–9 Credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, should develop a credit reporting code providing detailed guidance within the framework provided by the *Privacy Act* and the new *Privacy (Credit Reporting Information) Regulations*. The credit reporting code should deal with a range of operational matters relevant to compliance.

253 Rec 48–1.

55. More Comprehensive Credit Reporting

Contents

Introduction

55.1 This chapter presents recommendations to extend the current system of credit reporting to permit a broader spectrum of personal information to be collected and disclosed—referred to in this Report as 'more comprehensive' credit reporting.

55.2 The chapter begins by explaining what is meant by more comprehensive credit reporting and summarises the existing position on the content of credit information files and credit reports. The *Privacy Act 1988* (Cth), as explained in Chapter 53, restricts the types of personal information that may be collected and disclosed in the course of credit reporting. Broadly speaking, the Act mainly (but not exclusively) permits the collection and disclosure of personal information that detracts from an individual's credit worthiness—such as the fact that an individual has defaulted on a loan. This is commonly referred to as 'negative' or 'delinquency-based' credit reporting.

55.3 There has been a strong push by credit reporting agencies and credit providers to expand the types of personal information that may be collected and disclosed in the credit reporting process and, in particular, to permit the reporting of personal information relating to an individual's current credit commitments or repayment performance (or both).

55.4 This chapter examines the arguments for and against more comprehensive credit reporting, with particular reference to comments received in submissions and consultations, and information derived from empirical research into the possible effects of more comprehensive credit reporting on credit markets and the economy. The chapter also outlines some possible models of comprehensive credit reporting schemes, taking account of developments in other jurisdictions. For the reasons discussed in this chapter, the ALRC recommends that there should be an extension in the categories of personal information that may be collected for credit reporting purposes.

55.5 Any expansion in the categories of personal information that may be collected for credit reporting cannot be considered in isolation from other aspects of the regulation of credit reporting—for example, in relation to the data quality of credit reporting information, dispute resolution and penalties for the unauthorised use or disclosure of such information. These and other issues are discussed in Chapters 56–59 of this Report.

'Positive' or 'more comprehensive' credit reporting?

55.6 Much of the literature distinguishes between two distinct systems of credit reporting: 'negative' and 'positive' credit reporting.[1] The difference between these two sorts of credit reporting is said to lie in the kinds of personal information that can be collected as part of the credit reporting process. As the term suggests, negative credit reporting involves 'negative' information—that is, information that detracts from an individual's credit worthiness, such as the fact that he or she has defaulted on a loan. On the other hand, positive credit reporting is said to involve 'positive' information about an individual's credit position and includes information relating to that person's

1 See, eg, Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

current credit commitments. An example of information in this category is a record of an individual having made a loan repayment.

55.7 The terms 'negative' and 'positive' credit reporting are sometimes used as convenient shorthand expressions to distinguish between what is permitted under the current law (negative reporting) and what may be permitted if the current restrictions on reporting were relaxed (positive reporting). The use of the terms in this way involves a significant over-simplification because the credit reporting provisions currently permit the collection of some 'positive' items.[2]

55.8 More fundamentally, the term 'positive credit reporting' may be misleading because information collected through a positive credit reporting scheme can, in reality, be positive (in the sense of enhancing an individual's credit worthiness) or negative (that is, detracting from credit worthiness) depending on the particular situation. For example, 'data that is not default data can still be negative if it concerns missed payments or even very high levels of debt'.[3]

55.9 Therefore, a debate on whether 'positive' information should be included in credit reporting runs the risk of introducing a false premise—namely, that all information in this category would enhance the credit worthiness of the individual concerned. It is important that the debate be framed more clearly. As a result, the focus of this chapter is on whether it is appropriate to expand the categories of personal information involved in credit reporting and, if so, how.

55.10 Partly as a response to this semantic problem, some terms have been developed as alternatives to the term 'positive' credit reporting. The alternative term with the widest currency is 'comprehensive' credit reporting.[4] This term is preferable because it conveys more clearly that the information covered will not necessarily assist, nor hamper, an individual's application for credit. 'Comprehensive' in this context does not necessarily mean 'all' conceivable personal information of a financial nature that relates to an individual's credit worthiness. It is more appropriate, therefore, to talk about a *more comprehensive* system of credit reporting because this more accurately conveys the idea that what is being proposed is an expansion of the types of information a credit reporting agency can collect.

---

2 That is, a record of a credit provider being a current credit provider in relation to the individual: *Privacy Act 1988* (Cth) s 18E(1)(b)(v); a record of an enquiry made by a credit provider in connection with an application for credit, together with the amount of credit sought: s 18E(1)(b)(i).

3 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

4 See, eg, Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006). Another synonym is 'full-file reporting': see, eg, Consumers' Federation of Australia, *Full-File Credit Report: Is it Really the Answer to Credit Overcommitment?* (2005) <www.consumersfederation.com/documents/PositionPaperFeb05.doc> at 1 August 2007, 1.

55.11 While the use of the term 'positive' credit reporting has become prevalent in describing proposals to expand credit reporting in Australia, the ALRC considers that 'comprehensive' or 'more comprehensive' credit reporting represent clearer and more accurate short-hand expressions. Therefore, when the terms 'comprehensive' or 'more comprehensive' credit reporting are used in this chapter, they simply refer to a system of credit reporting that permits more types of personal information to be collected and used in credit reporting than is currently allowed under the *Privacy Act*.

Australia's approach to more comprehensive credit reporting

Current law

55.12 As discussed in more detail in Chapter 53, the credit reporting provisions of Part IIIA of the *Privacy Act* set out what information may be included in a credit information file. Section 18E(1) provides that a credit reporting agency may include information that identifies the individual in question and sets out an exhaustive list of the other categories of personal information that may be included in the file.[5] The information that may be contained in a credit information file includes a record of:[6]

- a credit provider having sought a credit report in connection with an application for credit, and the amount of credit sought (inquiry information);[7]
- a credit provider being a current credit provider in relation to the individual (current credit provider status);[8]
- credit provided by a credit provider to an individual, where the individual is at least 60 days overdue in making a payment on that credit;[9]
- a cheque for $100 or more that has been dishonoured twice;[10]
- a court judgment or bankruptcy order made against the individual;[11]
- a credit provider's opinion that the individual has committed a specific serious credit infringement.[12]

---

5 *Privacy Act 1988* (Cth) s 18E(1). In addition, *Privacy Act 1988* (Cth) s 18E(2) prohibits certain categories of personal information from being included in an individual's credit information file.

6 A more complete description of the permitted categories of personal information is contained in Ch 53.

7 *Privacy Act 1988* (Cth) s 18E(1)(b)(i). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

8 Ibid s 18E(1)(b)(v). The information may be kept for a maximum of 14 days after the credit reporting agency is notified that the credit provider is no longer the individual's credit provider: s 18F(2)(b).

9 Ibid s 18E(1)(b)(vi). The information may be kept for a maximum of five years after the credit reporting agency was informed of the overdue payment concerned: s 18F(2)(c).

10 Ibid s 18E(1)(b)(vii). The information may be kept for a maximum of five years after the second dishonouring of the cheque: s 18F(2)(d).

11 Ibid s 18E(1)(b)(viii), (ix). A record of judgment may be kept for a maximum of five years after the judgment was made: s 18F(2)(e). A record of a bankruptcy order may be kept for a maximum of seven years after the order was made: s 18F(2)(f).

55.13 With the exception of inquiry information[13] and current credit provider status,[14] this list contains mainly so-called negative information, such as information relating to the individual having defaulted on a loan. In effect, more comprehensive credit reporting is currently prohibited under the *Privacy Act*.[15]

55.14 There are many different models of more comprehensive credit reporting, as discussed below. Most jurisdictions that permit some form of more comprehensive credit reporting, however, include some or all of the following types of personal information:

- information about an individual's current loans or credit facilities, including the balances;
- an individual's repayment history;
- information about an individual's bank and other accounts, including the identity of the institution where the account is held and the number of accounts held; and
- further information than is currently permitted under the *Privacy Act* relating to overdue or defaulted payments.[16]

55.15 Reform to permit the collection and use of such categories of personal information in credit reporting would represent a significant extension of the current system in Australia.[17]

Government responses

55.16 Since the 1980s, both before and after the enactment of the credit reporting provisions, Australian federal and state governments have on several occasions considered the introduction of more comprehensive credit reporting.

---

12 Ibid s 18E(1)(b)(x). The information may be kept for a maximum of seven years after the information was included in the credit information file: s 18F(2)(g).

13 Ibid s 18E(1)(b)(i).

14 Ibid s 18E(1)(b)(v).

15 This prohibition derives from the interaction of ss 18E and 18K. Section 18K(2)(a) provides that a credit reporting agency must not disclose personal information if the information does not fall within the permitted categories in s 18E. Similarly, s 18E(8)(a) provides that a credit provider must not disclose personal information to a credit reporting agency if the information does not fall within the permitted categories in s 18E. These provisions are summarised in greater detail in Ch 53.

16 See, eg, Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 2.

17 The personal information that may be used currently in credit reporting is summarised in Ch 53.

Credit Reference Association of Australia proposal

55.17 As noted in Chapter 52, there was a push in the late 1980s for the introduction in Australia of a form of more comprehensive credit reporting. In that year, the Credit Reference Association of Australia (CRAA) stated its intention to collect information about individuals' current credit commitments.[18] This plan was postponed, however, at the request of the then Australian Government Minister for Consumer Affairs, the Hon Nick Bolkus.[19] Subsequently, the federal Parliament passed the *Privacy Amendment Act 1990* (Cth), which had the effect of prohibiting 'positive' credit reporting.

55.18 There were a number of concerns about the CRAA's proposal. The New South Wales Privacy Committee feared that the CRAA's proposal 'would greatly increase the quantity of personal information held by CRAA', and it may be too widely available.[20] The Australian Computer Society was concerned that this was 'an extremely privacy-invasive measure' demanding 'substantial justification'. It maintained that no detailed justification was publicly presented.[21]

55.19 Prior to the passage of the *Privacy Amendment Act 1990* (Cth), the then Minister for Consumer Affairs stated that one of the government's aims in passing this legislation was to 'tackle the whole question of positive reporting'. He noted that the government's rejection of 'positive reporting' was endorsed both by the Opposition and the Australian Democrats.[22] In the Second Reading Speech, the Minister went further, stating that so-called 'positive reporting' represents an unwarranted 'intrusion into individuals' lives' and that:

> The Government does not consider that there is any proven substantial benefit from the positive reporting proposals and that in view of the strong privacy concerns held by the community this massive expansion of the extent of information held about individuals should not be allowed to develop.[23]

Financial System Inquiry (Wallis Report)

55.20 The Financial System Inquiry, chaired by Mr Stan Wallis, discussed the issue of more comprehensive credit reporting in its 1997 final report (the Wallis report).[24] The Wallis report stated that the inquiry was not in a position to assess whether the benefits of positive credit reporting outweighed the costs, but considered the potential benefits warranted a complete review of the issue.[25]

---

18 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, [3.1].

19 New South Wales Government Privacy Committee, *Annual Report* (1989), 23.

20 Ibid, 22.

21 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, [3.2].

22 Commonwealth, *Parliamentary Debates*, Senate, 15 August 1989, 13 (N Bolkus—Minister for Consumer Affairs).

23 Commonwealth, *Parliamentary Debates*, Senate, 2 November 1989, 2788 (N Bolkus—Minister for Consumer Affairs).

24 Financial System Inquiry Committee, *Financial System Inquiry Final Report* (1997), 519–521.

25 Ibid, 521.

55.21 The Wallis report recommended that the Attorney-General should establish a working party, comprising representatives of consumer groups, privacy advocates, the financial services industry and credit reference associations to review the existing credit provisions of the *Privacy Act*. The purpose of this review should be to identify specific restrictions that prevent the adoption of world best practice techniques for credit assessment, and evaluate the economic loss associated with these restrictions against the extent to which privacy is impaired by their removal.[26]

Senate Legal and Constitutional References Committee

55.22 The inquiry undertaken in 2005 by the Senate Legal and Constitutional References Committee (Senate Committee privacy inquiry)[27] included consideration of credit reporting. Generally, the inquiry stated that while 'government action is required to maintain community confidence in [the] integrity of the credit reporting regime', it did 'not see any need for review or reform of Part IIIA at this time'.[28]

55.23 Specifically, the Senate Committee privacy inquiry recommended 'that the Privacy Act not be amended to allow the introduction of positive credit reporting in Australia'.[29] It explained this position by saying:

> The committee sees no justification for the introduction of positive credit reporting in Australia. Moreover, the experience with the current range of credit information has shown that industry has not run the existing credit reporting system as well as would be expected and it is apparent that injustice can prevail. As mentioned elsewhere in this report, positive reporting is also rejected on the basis that it would magnify the problems associated [with] the accuracy and integrity of the current credit reporting system. The privacy and security risks associated with the existence of large private sector databases containing detailed information on millions of people are of major concern.[30]

55.24 The Australian Government disagreed with the Senate Committee privacy inquiry's recommendation concerning credit reporting and stated that review of the credit reporting provisions is a matter that would be considered as part of the ALRC's inquiry.[31]

Senate Economics Committee

55.25 The Senate Economics Committee also considered the issue in its 2005 report *Consenting Adults, Deficits and Household Debt: Links between Australia's Current*

---

26 Ibid, rec 99.
27 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).
28 Ibid, [7.44]–[7.45].
29 Ibid, rec 17.
30 Ibid, [7.46].
31 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006).

Account Deficit, the Demand for Imported Goods and Household Debt.[32] The Committee stated that it was not persuaded to take a different view to that expressed by the Senate Legal and Constitutional References Committee.

> The Committee does not believe that credit providers are making full use of the information currently available to them. Further … defaults and other signs of financial distress in the credit card market are very low and do not justify the very significant change that would be required for positive credit reporting to be introduced. The Committee does not consider that any further parliamentary inquiry into this matter is justified at this time.[33]

Victorian Consumer Credit Review

55.26 Finally, the 2006 Victorian Consumer Credit Review (the Victorian Review) dealt with comprehensive credit reporting as part of a broad review of the efficiency and fairness of the operation of credit markets and the regulation of credit in Victoria.[34]

55.27 The Victorian Review received a large number of submissions on the benefits and limitations of the current system of credit reporting, and in relation to proposals to institute more comprehensive credit reporting. Ultimately, it concluded that a form of more comprehensive credit reporting should not be introduced, at least 'while substantial questions remain about whether the benefits outweigh the costs', and it suggested further research and analysis in this area.[35]

55.28 In its response to the review, the Victorian Government agreed that comprehensive credit reporting should not be implemented in Victoria on the ground that 'there is insufficient evidence' to show that it would be more beneficial than not to implement such a system. It went on to state that responsibility for 'further research and analysis' in this area should be borne by the Australian, as distinct from the Victorian Government.[36]

Regulation in other jurisdictions

55.29 As discussed above, the credit reporting provisions of Part IIIA provide an exhaustive list of the kinds of personal information that may be included in a credit information file or credit report. The collection of other kinds of information, including information about credit granted to individuals—such as credit limits or current balances—is not permitted.

---

32 Parliament of Australia—Senate Economics Committee, *Consenting Adults, Deficits and Household Debt—Links Between Australia's Current Account Deficit, the Demand for Imported Goods and Household Debt* (2005), [5.61]–[5.87].

33 Ibid, [5.87].

34 Victoria has its own legislation on credit reporting: *Credit Reporting Act 1978* (Vic). The Victorian Consumer Credit Review concluded that the Victorian legislation should be repealed because it has been superseded by the credit reporting provisions of the *Privacy Act 1988* (Cth): Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 280.

35 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 280.

36 Victorian Government, *Government Response to the Report of the Consumer Credit Review* (2006), 17.

55.30 How this aspect of credit reporting is regulated in other jurisdictions is considered in more detail below.[37] The following table compares, in summary, the information allowed in credit reports in Australia, New Zealand, Germany, Singapore, the United Kingdom (UK), Hong Kong, Canada, the United States (US) and Japan.[38]

Table 55–1 International Credit Reporting Information

	Bankruptcy	Court judgment	Default	Credit inquiries	Credit limit	Payment history	Employer	Account balance
Australia	√	√	√	√	–	–	–	–
New Zealand	√	√	√	√	–	–	–	–
Germany	√	√	√	–	√	–	–	–
Singapore	√	√	√	√	–	√	–	–
UK	√	√	√	√	√	√	–	–
Hong Kong	√	√	√	√	√	√	–	√
Canada	√	√	√	√	√	√	√	–
US	√	√	√	√	√	√	√	√
Japan	√	√	√	√	√	√	√	√

New Zealand

55.31 New Zealand is another jurisdiction in which more comprehensive credit reporting is effectively prohibited. In that jurisdiction, credit reporting is regulated by a binding code issued by the Privacy Commissioner under the *Privacy Act 1993* (NZ).[39]

37 Material on the regulation of credit reporting in other jurisdictions is drawn, in part, from: Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006).

38 This table is drawn, in part, from: Ibid, Table 2.4.

39 *Credit Reporting Privacy Code 2004* (NZ) under *Privacy Act 1993* (NZ) s 46.

55.32 The *Credit Reporting Privacy Code 2004* (NZ) (the NZ Code) provides that a credit reporting agency must not collect personal information for the purpose of credit reporting unless it is 'credit information'.[40] Briefly, credit information is defined exhaustively and includes identification information, information about credit applications, credit default information, judgment and bankruptcy information, serious credit infringements and information from public registers.[41]

55.33 While the information permitted by the NZ Code is in some respects broader than that permitted under Part IIIA,[42] the permitted content of credit reports closely replicates the position in Australia. Importantly, the NZ Code does not permit a credit reporter to collect information about an individual's current credit commitments and facilities.

United States

55.34 In the US, credit reporting is regulated under the *Fair Credit Reporting Act 1970* (US) (FCRA) by the Federal Trade Commission. The FCRA does not limit the permissible content of credit information files held by credit reporting agencies or the content of credit reports.[43]

55.35 Major credit reporting agencies in the US hold and report detailed information about individuals' credit accounts including, but not limited to, current balances, credit limits, amounts past due, payment performance and payment status pattern and account descriptions.[44] Credit reporting agencies receive information from credit providers and others, generally every month, and update their credit files within one to seven days of receiving new information.[45]

United Kingdom

55.36 In the UK, credit reporting agencies are regulated by both the *Consumer Credit Act 1974* (UK) and the *Data Protection Act 1998* (UK)—the latter being the equivalent of the Australian *Privacy Act*.

55.37 Neither the *Consumer Credit Act* nor the *Data Protection Act* specifically limits the permissible content of credit information files. The *Consumer Credit Act* deals only with individuals' rights of access to, and correction of, credit information about them.[46] Under the *Data Protection Act*, a 'data controller' (which may include a credit reporting agency) must comply with the data protection principles (DPPs) set out in the Act. These include DPP 3, which provides that 'personal data shall be adequate,

---

40 *Credit Reporting Privacy Code 2004* (NZ) r 1(2).
41 Ibid cl 5.
42 For example, the NZ Code allows the collection of 'information relating to identification documents reported lost or stolen or otherwise compromised' and 'credit scores': Ibid cl 5.
43 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US).
44 R Avery and others, 'An Overview of Consumer Data and Credit Reporting' (2003) (February) *Federal Reserve Bulletin* 47, 54.
45 Ibid, 49.
46 *Consumer Credit Act 1974* (UK) ss 157–160.

relevant and not excessive in relation to the purpose or purposes for which they are processed'.[47]

55.38 The information held by credit reporting agencies in the UK, and contained in credit reports, includes: data about the date accounts are opened; the credit limit or amount of the loan; payment terms; payment history; and payment arrangements entered into with the credit provider.[48] Unlike in the US, information on credit account balances is not collected.

Other jurisdictions

55.39 A 2006 report prepared for MasterCard Worldwide (MasterCard) summarised the key features of the regulatory systems for credit reporting in more than a dozen countries.[49] All the countries studied, with the exception of France, were said to permit more comprehensive credit reporting than in Australia.

55.40 A comparison was made of the kinds of information held by credit reporting agencies in Australia, the US, the UK, Germany, Canada, Japan, Hong Kong and Singapore.[50] This showed that in all countries except Australia, credit reporting agencies collect information about individuals' credit limits and payment history. In addition, credit reporting agencies in the US, Japan and Hong Kong also hold information about individuals' credit account balances.

55.41 Hong Kong implemented its regime of more comprehensive credit reporting in 2003, in part due to concern about levels of debt default and bankruptcy.[51] The Hong Kong Monetary Authority considered that the sharing by banks of more comprehensive information—through credit reporting agencies and subject to information privacy legislation—would help to promote a more effective banking system.[52]

---

47 *Data Protection Act 1998* (UK) sch 1, pt 1.

48 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 79; United Kingdom Government Information Commissioner's Office, *Data Protection: Credit Explained* (2006), 8, 13.

49 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006). The countries reviewed include the US, Canada, the UK, Germany, France, Italy, Belgium, South Africa, Japan, Hong Kong, South Korea, Singapore, Mexico and selected countries in Central and South America.

50 In some of these jurisdictions, credit reporting information is held by public credit registries rather than private sector credit reporting agencies. Public credit registries are operated by governments, usually banking and finance industry regulators that are similar, for example, to the Australian Prudential Regulation Authority: see Ibid, 9–11.

51 Ibid, 112.

52 Ibid, 112.

Lessons for Australia

55.42 Stakeholders that advocated more comprehensive credit reporting continued to contrast the position in Australia with that in jurisdictions overseas. For example, Veda Advantage noted that Hong Kong, Belgium, Greece, India and South Africa have all implemented models of more comprehensive reporting in the past five years.[53] American Express highlighted what it saw as the advantages of the systems in the US, UK, Hong Kong and Canada.[54]

55.43 While most other comparable jurisdictions permit credit reporting agencies to collect a broader spectrum of information than is permitted in Australia, this is not universally true. A number of jurisdictions—such as France, Spain and New Zealand—possess comparable restrictions to Australia in relation to the types of personal information that may be collected and used in credit reporting.[55]

The argument for more comprehensive credit reporting

55.44 The *Privacy Act* contains strict limitations on the categories of personal information that may be collected and used as part of the credit reporting process. These have been criticised by those advocating the introduction of more comprehensive credit reporting in Australia.

55.45 The underlying basis for criticism of the current credit reporting regime is that it does not do enough to allow credit providers to redress the information asymmetry between credit providers and potential borrowers.[56] As explained in Chapter 52, 'information asymmetry' refers to the situation where, because a credit provider often cannot know the full credit history of an individual applying for credit, the individual has more information about his or her credit risk than the credit provider. The greater the asymmetry, the harder it is for the credit provider to assess the risk premium associated with lending to the individual in question.[57]

55.46 The argument for reform of the current system of credit reporting is, in essence, that the current information asymmetry between credit providers and potential borrowers makes it unnecessarily difficult to assess the risk premium of individuals applying for credit. This, in turn, is said to cause a number of problems in assessing whether to provide credit:

---

53 Veda Advantage, *Submission PR 272*, 29 March 2007.

54 American Express, *Submission PR 257*, 16 March 2007.

55 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 12; J Peace, 'Knowing Your Customer: An Advantage for Business and Individuals?' (Paper presented at 28th International Conference of Data Protection Commissioners, London, 2 November 2006).

56 See, eg, ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 13–14.

57 The 'risk premium' reflects the costs associated with lending to a potential borrower. See, eg, Ibid, 2.

- It is difficult for a credit provider accurately to assess the risk involved in lending to an individual. This paucity of information can cause the credit provider to 'select some bad borrowers' (who default in their repayments) and to 'ignore some good ones' (who would have made their repayments had credit been extended to them).[58]

- While 'good borrowers have no way of signalling their reliability' to credit providers, 'bad borrowers have no incentive' to disclose their lack of credit worthiness.[59]

- When an individual has committed 'a minor default in the previous five years [this] can prevent access to affordable and serviceable credit', even when the individual's circumstances have changed. For instance, a person who defaulted on a payment for his or her mobile phone when he or she was under the age of 18 may be refused credit at a later stage—after he or she has entered the workforce and consequently represents a much lower credit risk.[60]

55.47 Due to problems in assessing the risk presented by individual borrowers, credit providers may charge borrowers an average interest rate that takes account of their experience of the pool of borrowers (good and bad) to whom they lend. This may cause adverse selection so that 'some good borrowers … drop out of the credit market', further increasing the average interest rate 'to cover the cost of loans that are not repaid'.[61]

Benefits of more comprehensive credit reporting

55.48 The ALRC has examined views on the advantages and disadvantages of more comprehensive credit reporting over the current credit reporting system, and on the economic and social impact of introducing a system of more comprehensive credit reporting in Australia.[62] In doing so, the ALRC consulted extensively with credit

---

58 Ibid, 2, 13–14.

59 Ibid, 14. See also Dun & Bradstreet, *Submission to Senate Economics Reference Committee Inquiry into Possible Links between Household Debt, Demand for Imported Goods and Australia's Current Account Deficit*, March 2005, 7.

60 Dun & Bradstreet, *Submission to Senate Economics Reference Committee Inquiry into Possible Links between Household Debt, Demand for Imported Goods and Australia's Current Account Deficit*, March 2005, 7. See also Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471,* 14 December 2007.

61 ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004); ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 17.

62 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 6–1, 6–2.

providers, credit reporting agencies, and consumer and privacy advocates; and received advice from a Credit Reporting Advisory Sub-committee.[63]

55.49 There are a number of possible benefits that may result from introducing comprehensive credit reporting. Some of the possible benefits are discussed below, with reference to views expressed in submissions.

Improved risk assessment

55.50 The starting point for many of the asserted benefits of more comprehensive credit reporting derive from the claim that it would improve the accuracy of credit risk assessment. The benefits said to flow from improved credit assessment include lower rates of over-indebtedness and default, greater competition in the credit market and less expensive credit. For example, it is said that the introduction of comprehensive credit reporting would increase the ability of credit providers to 'distinguish better between good and bad borrowers' and, in turn, reduce the rate of default and 'increase the volume of credit that can be provided to good borrowers'.[64]

55.51 Submissions from credit providers were virtually unanimous in suggesting that more comprehensive credit reporting has the potential to enhance credit risk assessment significantly.[65]

> There is a general consensus amongst credit and risk professionals that the sharing of more information should lead to better decisions. When coupled with good regulatory protections for consumers the outcome is a robust and well balanced credit market.[66]

55.52 GE Money Australia stated that:

> Our experience in a number of international markets is that comprehensive or 'positive' credit bureau data adds significantly to our ability to accurately assess an applicant's credit risk. This improved capability enables us to more accurately assess risk, which can in turn reduce credit losses (including fraud losses), a cost that is ultimately borne by consumers.[67]

---

63 The process of reform is described in Ch 1.

64 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 19, 21. See also Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 7.

65 See, eg, GE Money Australia, *Submission PR 537,* 21 December 2007; Westpac, *Submission PR 472,* 14 December 2007; ANZ, *Submission PR 467,* 13 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Australian Finance Conference, *Submission PR 398,* 7 December 2007; Confidential, *Submission PR 297,* 1 June 2007; Australian Finance Conference, *Submission PR 294,* 18 May 2007; ANZ, *Submission PR 291,* 10 May 2007; Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

66 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

67 GE Money Australia, *Submission PR 233,* 12 March 2007.

55.53 Stakeholders contrasted the predictive value of the information currently available to that available under more comprehensive credit reporting systems and submitted that inadequate data sharing under existing arrangements leads to problems of adverse selection and moral hazard.[68]

> Credit providers are currently only able to rely on information supplied by application, together with negative information provided in a credit report. If an applicant fails to disclose facilities they hold with other financial institutions, the credit provider is unable to make a fully informed lending decision resulting in the possibility of provision of credit to borrowers who are unable to meet their financial obligations.[69]

55.54 In contrast, through the application of more comprehensive information a lender is able to 'detect those individuals comprising the pool of high risk potential debtors'.[70]

> When overall levels of the borrower's obligations are provided as part of the 'positive data' then less reliance is needed on the incomplete data provided in negative only data environments. Lenders can then use the full picture of a consumers' indebtedness and their previous payment history to make a much more informed assessment of risk and hence a more responsible lending decision.[71]

55.55 In this context, industry stakeholders presented a range of findings concerning the relative value of various possible data items in predicting lending risk. These findings are discussed later in this chapter.

Promoting competition and efficiency

55.56 Comprehensive credit reporting is also said to promote competition in credit markets. Among other things, more competition may mean that credit is more readily available, at lower cost, and in more forms than would otherwise be the case.

55.57 A 2004 report commissioned by MasterCard (the MasterCard/ACIL Tasman Report) stated that, for example, following increases in the types of personal data collected and used in credit reporting in the US in the 1980s and 1990s, there was 'a wave of new entrants into the bank credit card market'. This led to 'downward pressure on interest rates and fees for bank credit cards' and 'the introduction of differential pricing in bank credit cards … with lower interest rate margins for lower risk borrowers', and an overall expansion in the credit card market.[72] In response, it may be

---

68 The meaning of these terms is discussed in Ch 52.

69 National Australia Bank, *Submission PR 408,* 7 December 2007.

70 American Express, *Submission PR 257,* 16 March 2007.

71 Veda Advantage, *Submission PR 272,* 29 March 2007.

72 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 31. There was a 'similar expansion' in mortgages and personal loans for motor vehicles: ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 32.

observed that many of these developments also occurred in countries where there were no similar changes to credit reporting—including Australia.

55.58 In the Australian context, Abacus–Australian Mutuals (Abacus) noted that the ability of larger credit providers to use internal databases of 'positive' credit data relating to their own customers offers a potential competitive advantage in assessing credit risk. More comprehensive reporting may help create more competitive markets, because consumers are less reliant on existing institutional relationships to obtain credit.[73]

55.59 Other submissions also referred to the promotion of more competitive credit markets.[74] For example, Dun and Bradstreet (Australia) Pty Ltd stated that

> improved data sharing is critical to the efficient operating of credit markets, resulting in improved products and rates for consumers and more efficient pricing for credit providers.[75]

55.60 Veda Advantage considered that more comprehensive reporting promotes competition in credit markets 'by reducing information barriers for small or new credit providers'.[76]

55.61 Stakeholders noted the possible role of more comprehensive credit reporting in reducing the transaction costs involved in assessing credit applications. For example, Experian Asia Pacific considered that more comprehensive credit reporting could facilitate more automation and 'faster decisions' in credit and other financial services transactions.[77]

55.62 The need for reform of credit reporting to maintain 'competitive neutrality' among credit providers was highlighted.[78] If more comprehensive credit reporting were introduced in Australia, this would also have a significant impact on the credit reporting market. For instance, it is said that this would enhance the capacity for competition between credit reporting agencies.[79] This should make it easier for relative

---

73 Abacus–Australian Mutuals, *Submission PR 278*, 10 April 2007.

74 HBOS Australia, *Submission PR 475,* 14 December 2007; ANZ, *Submission PR 467,* 13 December 2007; ANZ, *Submission PR 291,* 10 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

75 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

76 Veda Advantage, *Submission PR 272,* 29 March 2007.

77 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

78 MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007.

79 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 20. See, generally, ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 36.

newcomers in the Australian credit reporting market to increase their market share more rapidly.

55.63 Reference was made to the fact that the existing credit reporting provisions may operate as a barrier to new entrants into the credit reporting market and hinder competition.[80] The reasons for this view include that it takes a long period of time to develop databases of 'negative' events, such as defaults on loans; and complex and prescriptive legislative requirements increase the cost to a new entrant of developing the information technology infrastructure needed to conduct consumer credit reporting. The benefits of competition between credit reporting agencies might include improved data accuracy and a greater range of related services available to individuals and credit providers.[81]

55.64 Greater competition and efficiency in credit markets may have a range of flow-on benefits for individual consumers, such as lowering the cost of credit, increasing the availability of credit and reducing default rates.

55.65 Some argue that, by ensuring greater accuracy in risk assessment and management for credit providers, comprehensive credit reporting could help reduce the cost of credit for individuals—particularly for those who are a low credit risk.[82] By allowing credit providers to assess risk more accurately, it would 'increase their scope to set interest rates to reflect the risk premiums associated with different types of borrowers'.[83] National Australia Bank, for example, stated:

> Applicants who fail to disclose their true financial position create disproportional risks to credit providers which are subsidised by other borrowers. More comprehensive reporting will improve the veracity of credit information, enhance risk-based pricing and result in a fairer distribution of credit.[84]

55.66 A number of credit providers confirmed that more comprehensive credit reporting has the potential to lead to lower cost credit.[85] This outcome was attributed to the likely effects of increased competition among credit providers;[86] reduced credit

---

80 GE Money Australia, *Submission PR 233,* 12 March 2007.

81 Ibid.

82 ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004), 3; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 11,* 13 April 2006, Annexure (Briefing Note), 4.

83 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 20.

84 National Australia Bank, *Submission PR 408,* 7 December 2007.

85 HBOS Australia, *Submission PR 475,* 14 December 2007; ANZ, *Submission PR 467,* 13 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; American Express, *Submission PR 257,* 16 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

86 GE Money Australia, *Submission PR 233,* 12 March 2007.

provider costs associated with the risk assessment process;[87] and the reduced cost of bad debts.[88] Another possible effect of more comprehensive reporting may be to increase access to credit, especially among low income earners.[89]

55.67 Consumer groups expressed concern about possible lending and credit pricing practices that might be facilitated by more comprehensive reporting. The Consumer Credit Legal Centre (NSW) (CCLC) submitted, for example, that the 'use of credit file information to trigger price variations on existing contracts should be expressly prohibited' and warned that an enhanced ability on the part of credit providers to price risk 'should not be accepted as being necessarily in the public interest'.[90] Galexia Pty Ltd (Galexia) expressed concern about whether more information would lead to a range of undesirable credit marketing practices that are 'entrenched elements of some jurisdictions where positive credit reporting is allowed'.[91]

Effects on the credit market and lending practices

55.68 One of the claimed benefits of more comprehensive credit reporting is that it can reduce levels of over-indebtedness and default because credit providers will be in a better position to gauge when credit should be refused. However, some have challenged this proposition.

55.69 In response to the claimed link between the categories of personal information available to credit providers and overall levels of indebtedness, the Victorian Review cited research carried out in 2003 by Nicola Jentzsch and Amparo San José Riestra. This research found that evidence from the European and US markets does not support the argument that there is a relationship between the existence of comprehensive credit reporting and lower levels of indebtedness.[92]

55.70 The Victorian Review suggested that, if this conclusion is correct, it throws into doubt whether more information in a credit report can assist in managing risk or aid responsible lending.[93] The Consumers' Federation of Australia (CFA) also has argued that, rather than comprehensive credit reporting decreasing the number of individuals defaulting on repayments, it is 'likely to increase the number of consumer credit

---

87 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 11,* 13 April 2006, Annexure (Briefing Note), 4.

88 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

89 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; St George Banking Limited, *Submission PR 271,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

90 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

91 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

92 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 274, citing N Jentzsch and A San José Riestra, *Information Sharing and Its Implications for Consumer Credit Markets: United States vs Europe* (2003) European University Institute <www.iue.it/FinConsEU/ResearchActivities/EconomicsOfConsumerCreditMay2003> at 5 May 2008, 13.

93 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 274.

defaults'.[94] The CFA maintained that research conducted by US economists Professors John Barron and Michael Staten (the Barron and Staten research), relied on by a number of the advocates of comprehensive credit reporting, is equivocal on this point,[95] and that comprehensive credit reporting may result in either greater availability of credit (with the current rate of default) or a lower rate of default (with a correspondingly lower availability of credit), but not both.[96]

55.71 This interpretation was restated in submissions to the Inquiry by consumer groups.[97] The Consumer Action Law Centre stated that the actual outcome of more comprehensive reporting will depend on whether credit providers choose to reduce default rates or to advance more credit and that the latter outcome is more likely—leading ultimately to more default and bankruptcy.[98]

55.72 MasterCard submitted that it is a misinterpretation of the Barron and Staten research to suggest that more comprehensive reporting may lead to either a lower default rate or more availability of credit with the same default rate (but not both). MasterCard stated that, while the actual levels of default and credit availability modelled cannot be achieved simultaneously (given the research assumes holding one parameter constant when modelling the impact of change to the other measure), lower default rates and greater availability of credit 'are not mutually exclusive' outcomes. Rather, 'the Australian credit marketplace will find a natural balance'.[99] Some credit providers conceded that the overall level of indebtedness is likely to rise, even though the overall proportion of bad loans would decline.[100]

Responsible lending

55.73 Submissions in support of more comprehensive credit reporting also focused on its possible role in reducing default rates and encouraging 'responsible lending' practices.[101] Responsible lending can be defined in different ways and is manifested in

---

94 Consumers' Federation of Australia, *Full-File Credit Report: Is it Really the Answer to Credit Overcommitment?* (2005) <www.consumersfederation.com/documents/PositionPaperFeb05.doc> at 1 August 2007, 1.

95 See J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 5 May 2008.

96 Consumers' Federation of Australia, *Full-File Credit Report: Is it Really the Answer to Credit Overcommitment?* (2005) <www.consumersfederation.com/documents/PositionPaperFeb05.doc> at 1 August 2007, 2. A similar point is made in Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

97 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

98 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

99 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

100 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007. GE Money stated that there is no proof that more comprehensive reporting would increase levels of indebtedness: GE Money Australia, *Submission PR 537,* 21 December 2007.

101 Veda Advantage, *Submission PR 498,* 20 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; Abacus–Australian Mutuals, *Submission PR 456,* 11 December 2007; National

different institutional policies and practices.[102] The basic obligations of responsible lending include that credit providers should lend only what their customers can afford to repay, help to prevent over indebtedness, and market their products and services responsibly.[103]

55.74 Credit providers also have legal obligations not to provide credit where capacity to repay has not been reasonably established. In particular, under s 70 of the *Consumer Credit Code*,[104] a court may reopen an unjust transaction.[105] In determining whether a transaction is unjust, the court may have regard to, among other things, whether 'the credit provider knew, or could have ascertained by reasonable inquiry of the debtor at the time, that the debtor could not pay'.[106]

55.75 At least in theory, a better understanding of a credit applicant's existing financial obligations should assist credit providers to avoid lending to those who are over-committed and to intervene to manage existing customers who become over-committed. More comprehensive credit reporting is said to place the onus on the credit provider to ensure responsible lending, rather than relying on the borrower to reveal their existing commitments, which applicants often fail to disclose fully.[107]

55.76 In submissions, consumer groups expressed continued concern about the actual impact on the credit market of more comprehensive reporting—particularly in the absence of a 'specific legislative requirement upon all credit providers to lend responsibly having regard to all reasonably accessible data'.[108] Consumer groups are not confident that more comprehensive reporting would automatically result in more responsible lending decisions.

55.77 The CCLC stated that current casework experience 'suggests that the improvement in responsible lending predicted by the credit reporting agencies will not

---

Australia Bank, *Submission PR 408,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007; St George Banking Limited, *Submission PR 271,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

102 See, eg, Westpac Banking Corporation, *Principles of Responsible Lending* (2007) <www.westpac.com .au/internet/publish.nsf/Content/WICRCU+Responsible+lending> at 5 May 2008.

103 Ibid.

104 The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories.

105 *Consumer Credit Code* s 70(1).

106 Ibid s 70(2)(l).

107 National Australia Bank, *Submission PR 408,* 7 December 2007. Research conducted for Veda Advantage found that 'as many as 2.7 million Australians have lied on a credit application form to get credit': Veda Advantage, *Submission PR 498,* 20 December 2007. The research was undertaken by Galaxy Research in September 2007 and is based on a telephone survey of 1,100 households.

108 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 133. The CCLC recommended that stand-alone responsible lending provisions should be introduced into the *Consumer Credit Code*, requiring credit providers to take reasonable steps to ensure that an applicant can meet his/her obligations under the contract without substantial hardship: Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 58.

occur as a consequence of an extended credit reporting system but would have to be specifically imposed by the legislature'.[109] The Australian Privacy Foundation considered that:

> no convincing evidence has been produced to support the claim that more information would be used to lend more responsibly rather than to increase the total amount of lending. In the absence of better regulation of lending practices, (and especially in the current economic environment), the Australian community cannot take the risk that more comprehensive credit reporting would not be used irresponsibly, with the potential for significant harm not only to individuals but also to the overall economy.[110]

55.78 The Uniform Consumer Credit Code Management Committee (UCCCMC) agreed that it remained unclear what actual impact more comprehensive reporting would have on lending practices. The UCCCMC noted that the Ministerial Council on Consumer Affairs has an 'in-principle interest' in tools—such as more comprehensive reporting—that 'can enhance assessment of capacity to repay as it can, in theory, promote responsible lending'.[111]

55.79 It was noted in submissions that more comprehensive credit reporting would enhance the ability of credit providers to comply with responsible lending obligations. For example, MasterCard stated that more accurate information on a credit applicant's capacity to repay would make the *Consumer Credit Code* a much more effective tool 'to prohibit over-extension, or impose sanctions on those [who] breach such prohibitions'. MasterCard submitted that consumer groups should, on that basis, lobby for the introduction of compulsory comprehensive credit reporting in Australia 'in much the same way that their counterparts in the UK are outspoken supporters of positive credit reporting there'.[112]

55.80 Consumer groups and others were sceptical about claims that more comprehensive reporting would be used to promote responsible lending, at least in the absence of positive legislative obligations.[113] Legal Aid Queensland submitted:

> [T]here is insufficient evidence to predict that this extra information would be used by industry to lend responsibly … Even the industry players … have conceded that the overseas experience does not support either more responsible lending or a decrease in defaults. The only claim is that the percentage of bad loans would fall.[114]

---

109 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

110 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

111 Uniform Consumer Credit Code Management Committee, *Submission PR 520,* 21 December 2007.

112 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

113 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; National Legal Aid, *Submission PR 521,* 21 December 2007; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

114 Legal Aid Queensland, *Submission PR 489,* 19 December 2007.

55.81 The Consumer Action Law Centre, in opposing more comprehensive reporting, stated that while access to additional information in credit reports would improve credit providers' ability to assess risk, 'we fear this could be used as much to increase irresponsible and exploitative lending as it would to achieve "responsible lending" objectives'.[115] Similarly, the Cyberspace Law and Policy Centre stated:

> In our view there remains insufficient evidence that any extra information would be used responsibly to the benefit of individuals, and no guarantees that it will not instead be used to increase the total volume of lending, and to target different classes of borrower and loans in ways which would contribute to over-commitment and financial stress.[116]

55.82 The Australasian Retail Credit Association (ARCA), a peak body of credit providers and credit reporting agencies interested in the operation and reform of the credit reporting system, claimed that more comprehensive credit reporting would increase levels of 'financial literacy'[117]—the knowledge necessary for individuals to make informed decisions about the management of their personal finances—which in turn assists credit providers to lend responsibly. Arguably, individuals in jurisdictions that have systems that record 'positive' information about credit history are more aware of their 'credit rating' and the consequences of late payments or default. Individuals also have more potential to improve their credit record after a default by subsequently establishing a solid repayment history.[118] In Australia, by comparison, many individuals are not even aware of the credit reporting system unless they have actually been refused credit as a result of information in their credit information file.

Problems with more comprehensive credit reporting

55.83 Those against introducing more comprehensive credit reporting challenge some of the claimed benefits, as discussed above. In addition, it is argued that any benefits from the introduction of comprehensive reporting are likely to be outweighed by concerns about information privacy and security.

Impact on privacy and security of personal data

55.84 There is disquiet about the impact of comprehensive credit reporting on an individual's right to privacy. Various government inquiries have expressed concern in this regard.[119] The Victorian Review noted that a system of more comprehensive credit reporting would have a significant 'potential impact on privacy … particularly in relation to financial matters'.[120]

---

115 Consumer Action Law Centre, *Submission PR 510,* 21 December 2007.
116 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.
117 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007: see also GE Money Australia, *Submission PR 233,* 12 March 2007.
118 GE Money Australia, *Submission PR 233,* 12 March 2007.
119 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.46].
120 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 273.

55.85 Telstra Corporation Ltd (Telstra) stated simply that 'it is by no means clear that more comprehensive credit reporting would provide additional benefit outweighing the additional exposure to an individual's privacy'.[121] Other stakeholders elaborated privacy concerns about more comprehensive reporting. The CCLC, for example, submitted that more comprehensive credit reporting 'is fraught with privacy and security risks', particularly given that it will likely entail 'a large database of information about millions of people [being] maintained by one or more third parties'. In particular, the CCLC was concerned about data accuracy, and misuse for marketing and other unauthorised purposes, including identity fraud.[122]

55.86 Veda Advantage characterised the privacy risks as involving: first, the risk to the individuals arising from a more significant quantity of data about them being held and shared among credit providers; and secondly, the potential harms arising from the misuse of the data, for both credit and non-credit related purposes. Concerns were expressed about the possible use and disclosure of credit information for non-credit related purposes.[123] National Legal Aid, for example, stated:

> Our concerns in relation to the proposed expansion of the contents of a credit report are related to the continuation or expansion of the organisations that have access to the main consumer credit reporting databases. The risk is too great that comprehensive information about individuals' finances will be used for a range of purposes that go beyond simply assessing the creditworthiness of an applicant for credit.[124]

55.87 The accuracy of the information collected under a more comprehensive credit reporting system was another focus of concern in submissions.[125] The Office of the Privacy Commissioner (OPC) submitted that expanding the volume and depth of information that would be available on individuals' credit information files 'may worsen the current problems with accuracy of credit information'.[126] Galexia expressed specific concerns about the accuracy of repayment performance information,[127] which may be affected by requiring credit providers 'to provide more information, requiring more data entry and more opportunities for errors'; and because credit providers 'may not have the same motivation to check the accuracy of data (especially disputed data) as they do to check default data in traditional credit reporting information, as the consequences of an inaccuracy will appear less severe'.[128]

---

121 Telstra Corporation Limited, *Submission PR 459,* 11 December 2007.
122 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.
123 Issues concerning regulation of the use and disclosure of credit reporting information, including any personal information additional to that currently permitted, are discussed in more detail in Ch 57.
124 National Legal Aid, *Submission PR 521,* 21 December 2007.
125 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
126 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
127 Such as the information proposed to be collected under the ARCA proposal (discussed in detail below).
128 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

55.88 In contrast, credit reporting agencies and some credit providers believed that more comprehensive credit reporting should result in improved accuracy of data.[129] These improvements would result from more frequent and automated reporting[130] (depending on the model of reporting implemented) and more consumer engagement with credit information files.[131] The chances of inaccuracies affecting decisions about granting credit may be reduced because of the presence of other data.[132] For example, the impact of one late payment on an individual's credit score may be mitigated by the balance of that individual's overall repayment history.

55.89 Data security was also cited as a privacy concern. Reference was made to incidents overseas where the security of comprehensive credit reporting information has been compromised by credit reporting agencies.[133]

55.90 Finally, there was concern about the appropriateness of credit reporting agencies collecting and reporting payment performance information in relation to utilities, such as telecommunications, energy and water.[134] The Telecommunications Industry Ombudsman noted that there 'are numerous reasons why a customer may not be able to pay their bill on time, many of which do not equate to the customer being a potential credit risk'.[135]

55.91 Submissions from those in favour of more comprehensive credit reporting indicated that the proponents are well aware of these and other privacy concerns. American Express stated, rather than being insurmountable, privacy concerns can be addressed through 'the imposition of legislative controls or general prohibitions on the use of information', strengthened enforcement and more flexible penalties.[136]

55.92 Proponents agree that, if a more comprehensive credit reporting system is to be implemented, there needs to be a range of improvements to the present regulatory regime. These improvements—many of which are desirable whether or not there is a move toward more comprehensive reporting—are discussed in detail in Chapters 56–59.

---

129 ANZ, *Submission PR 291,* 10 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007.

130 Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007.

131 Veda Advantage, *Submission PR 272,* 29 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007. Under some models of more comprehensive reporting, what is reported to the credit reporting agency will be reflected on the individual's statement of account, greatly reducing the incidence of incorrect default listings: GE Money Australia, *Submission PR 233,* 12 March 2007.

132 Veda Advantage, *Submission PR 272,* 29 March 2007.

133 Westpac, *Submission PR 256,* 16 March 2007.

134 Energy and Water Ombudsman NSW, *Submission PR 225,* 9 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

135 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007. For example, customers may have received an unexpectedly high bill due to inadequate management of utilities provision.

136 American Express, *Submission PR 257,* 16 March 2007.

Empirical studies

55.93 Proponents claim that empirical studies provide important evidence about the likely credit market efficiency and economic benefits of more comprehensive credit reporting. A number of studies have been referred to in submissions and consultations. These and other relevant studies are discussed briefly below.

Credit market efficiency

55.94 The research most commonly cited in this context is the Barron and Staten research,[137] published in 2000.[138] Barron and Staten compared the position of credit providers in relation to risk assessment under the rules provided by the FCRA in the US and the *Privacy Act* respectively, using US data provided by Experian Information Solutions Inc, a leading US credit reporter. The research compared the accuracy of risk scoring models using the credit reporting variables available under the US system with the more limited set of variables available in Australia.

55.95 The research found that the more comprehensive form of credit reporting would enable credit providers to achieve a lower rate of defaults on loans, while maintaining the same loan approval rate (for example, at an approval rate of 60%, the Australian variables produced a default rate of 3.35%, as compared to 1.9% for the US variables). At the same time, assuming that default rates were maintained at the same rate (for example, 4%), credit providers using the Australian variables would extend new credit to 11,000 fewer consumers for every 100,000 applicants than would be the case if they were allowed to use the more comprehensive data available under US law.[139]

55.96 Later research by Barron and Staten, conducted at the request of the Australian Finance Conference (AFC), compared the effect of the US variables with an 'intermediate model' of credit reporting that allows for the reporting of the 'existence (and type) of accounts that are in good standing or have been paid in full, but does not report current balances or revolving account credit limits'.[140] This 2007 research found that, at the targeted approval rate of 60%, the intermediate model produced a 2.46% default rate.[141]

---

137 The Barron and Staten research was referred in: Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

138 J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 5 May 2008.

139 Ibid, 20. The more comprehensive credit reporting model would approve 83% of applicants compared to 74% of applicants using the more restricted information.

140 M Staten and J Barron, *Positive Credit Report Data Improves Loan Decision-Making* (2007) Australian Finance Conference.

141 Ibid.

55.97 The implications of the Barron and Staten research are said to include that consumer credit will be less available and more expensive in countries (such as Australia) where credit reporting omits categories of variables that would provide a more complete picture of a consumer's financial position.[142]

55.98 Other evidence about the benefits of more comprehensive reporting is said to derive from studies that compare credit reporting regimes in different jurisdictions with the characteristics of the credit markets in those jurisdictions. For example, Tullio Jappelli and Marco Pagano analysed the credit reporting regimes and credit markets in 43 countries, including the US, Australia and most other Organisation for Economic Co-operation and Development countries. Their econometric analysis found that the breadth and depth of a credit market was positively associated with the extent of the credit information that was exchanged between lenders.[143]

55.99 In 2003, a US Congressional Research Service report surveyed the literature (including that already discussed) and concluded that empirical research suggested that privacy laws that restrict the reporting of consumer credit data could lead to the potential loss of significant economic benefits. That is, credit data limitations may increase the cost of consumer credit, reduce accessibility and lower the overall volume of lending.[144]

55.100 There is debate about the conclusions that may be drawn from empirical studies of the effects of more comprehensive credit reporting on credit markets in view of methodological limitations and the assumptions built into research models. For example, it may be observed that the Barron and Staten research—in comparing the accuracy of credit scoring using variables available under the US system with the more limited set of variables available in Australia—disregarded the 'positive' information provided on application forms.

> Their results are not directly comparable to actual experience in the Australian market, because they do not factor in the additional (though limited) predictive value of the additional demographic data that Australian lenders generally use to make up that difference.[145]

55.101 The Victorian Review noted that, in order to consider fully the possible benefits of more comprehensive reporting in assessing capacity to repay, research would need to show a material gap between the information provided by the consumer and the information in a more comprehensive credit report. That is, whether the information sourced directly from consumers

---

142 J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 5 May 2008, 28.

143 T Jappelli and M Pagano, *Information Sharing, Lending and Defaults: Cross-Country Evidence* (2000) Centre for Studies in Economics and Finance, University of Salerno. The Jappelli and Pagano research was referred to in: MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

144 L Nott, *The Role of Information in Lending: The Cost of Privacy Restrictions* (2003), 9.

145 GE Money Australia, *Submission PR 233,* 12 March 2007.

> is materially less helpful to assessing capacity to repay than that from a positive credit reporting agency having regard for:
>
> - weight given to negative information rather than positive information generally;
> - existing capacity to verify positive information, albeit through a more costly process of having to contact other credit providers individually;
> - likely inaccuracies in the data;
> - the potential use of profit scoring[146] mechanisms;
> - other factors independent of this information that may be more material to repayment capacity, such as loss of job, death/separation from spouse, etc.[147]

55.102 Submissions to this Inquiry referred to the experience in a range of other countries as support for the view that the introduction of more comprehensive reporting would have significant benefits for credit markets.

55.103 Dun and Bradstreet referred to data from Japan, Hong Kong and Latin America (in addition to placing reliance on the Barron and Staten research). For example, it was said that Hong Kong experienced a dramatic decline in loan defaults following the introduction of more comprehensive reporting in 2002.[148] MasterCard, American Express and Veda Advantage also referred to the Hong Kong experience.[149] Veda stated:

> Australia should act earlier and more decisively than in Hong Kong, where a negative credit reporting regime failed to prevent a huge surge in consumer bankruptcies amid similar credit tightening in 2002. More comprehensive credit reporting was then introduced and helped consumers and their lenders manage risk better, with a halving of bankruptcies by 2004, and a further 90% reduction by 2006.[150]

55.104 An important qualification in drawing any conclusions from this experience may be that Hong Kong's economy began to recover from a recession in this period, and it is possible that this recovery was a more important cause of the decline in loan

---

146 'Profit scoring' essentially refers to a score that takes into account profits generated from late payments, for example, rather than the actual risk. Accordingly, risk reduction may compete with profit scoring: Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 261.

147 Ibid, 260. In April 2005, ANZ conducted a trial of completed statements of financial position provided by customers applying for a credit limit increase in the ACT. The study found that 24% of forms had errors and omissions in financial details: ANZ, *Submission PR 291,* 10 May 2007.

148 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

149 Veda Advantage, *Submission PR 498,* 20 December 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007. MasterCard Worldwide claimed that, in Hong Kong, material defaults by individuals fell by 27% following the introduction of comprehensive credit reporting: MasterCard Worldwide, *Submission PR 237,* 13 March 2007. See also Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 17.

150 Veda Advantage, *Submission PR 498,* 20 December 2007.

defaults than credit reporting reform. More generally, different macro-economic environments limit the applicability of conclusions drawn from international experience about the possible effects of more comprehensive reporting on levels of default, credit availability and interest rates in Australia. There are many factors, relating to credit markets and macro-economic conditions generally, which have an influence on these outcomes.

55.105 Some studies cast doubt on the relationship between more comprehensive credit reporting and credit market efficiency. Jentzsch and San José Riestra created a 'credit reporting regulatory index' for 27 jurisdictions in Europe and the US, which measured the extent of information privacy regulation affecting credit reporting. Their research found that, while increased coverage of credit reporting (in terms of the number of credit reports issued scaled by population) is associated with increased access to credit, there was no evidence that privacy restrictions greatly hampered information sharing in consumer credit markets.[151]

Macro-economic benefits

55.106 Research also has modeled the macro-economic impact of introducing more comprehensive credit reporting in Australia.[152] The MasterCard/ACIL Tasman report concluded that comprehensive credit reporting would generate a one-off increase in capital productivity of 0.1%, which would translate to economic benefits to the Australian economy of up to $5.3 billion, in net present terms, over the next 10 years.[153]

55.107 ACIL Tasman used what was described as an 'applied general equilibrium model' of the Australian and world economies to quantify the benefits of more comprehensive credit reporting. The model assumed that 'the efficiency of the credit market has implications for the efficiency of virtually every sector of the economy',[154] and took as one starting point the Barron and Staten findings about the possible reduction in the rate of default if a US-style comprehensive reporting system were adopted.[155]

55.108 As with research about credit market effects, there are methodological limitations built into research into the macro-economic impact of credit reporting

---

151 N Jentzsch and A San José Riestra, 'Consumer Credit Markets in the United States and Europe' in G Bertola, R Disney and C Grant (eds), *The Economics of Consumer Credit* (2006) 27, 51.

152 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004). The ACIL Tasman research was referred to in: MasterCard Worldwide, *Submission PR 237*, 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

153 ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004), 3. See also ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 28.

154 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 3.

155 Ibid, 24.

systems. On one view, the subject matter does not lend itself to precise modelling due to the level of complexity and the small orders of magnitude involved in terms of benefits. It is questionable whether any modelling will provide definitive answers. For example, Australia is recognised as having a credit market that is very competitive by international standards. This may limit the potential for further competitive gains resulting from more comprehensive reporting. Equally, a macro-economic upturn seems likely to have a much greater influence on credit availability than any change to a credit reporting system.

Models of more comprehensive credit reporting

55.109 There is a spectrum of views about the categories of personal information that should be able to be collected as part of a more comprehensive credit reporting system. In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC identified a lack of consensus regarding a preferred model of comprehensive reporting.[156] In the past, this has hindered debate about whether more comprehensive reporting should be introduced, including in the context of previous government inquiries.[157] More recently, a significant number of credit providers have reached broad agreement on the desirable elements of a more comprehensive credit reporting system, including on the categories of personal information that should be collected.

New categories of personal information

55.110 An important focus of the Inquiry has been on whether Australian law should be amended to expand the categories of personal information that may be collected and used in credit reporting and, if so, what categories of personal information should be permitted. The following discussion focuses only on categories of personal information that concern an individual's current credit commitments or repayment performance. Chapter 56 deals with the collection of other categories of personal information, such as identifying information.

55.111 In response to the Issues Paper, *Review of Privacy—Credit Reporting Provisions* (IP 32),[158] a range of views was expressed, from those suggesting loosening prohibitions on the content of credit reporting information through to those suggesting only minor extensions to the content currently permitted under s 18E of the *Privacy Act*.

---

156 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [51.117].

157 See, eg, Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 273. In its response to the Victorian Review, the Victorian Government observed that this lack of consensus makes it difficult to determine whether more comprehensive credit reporting would in practice 'enhance decision making' by credit providers: Victorian Government, *Government Response to the Report of the Consumer Credit Review* (2006), 46.

158 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006).

55.112 Some credit reporting agencies and credit providers favoured removing the existing restrictions and permitting the collection of an extensive range of information about accounts, repayment performance and current credit commitments.[159] An alternative approach, proposed by Dun and Bradstreet, would permit credit reports to contain a limited number of additional data elements only, including information identifying an individual's open accounts and credit limits.[160] Some credit providers considered that these categories of information were the minimum necessary to deliver benefits in credit decision making. On the other hand, this more limited model of more comprehensive reporting was criticised by others in the credit industry, primarily because it 'lacks the most predictive risk data that is the repayment history'.[161]

Discussion Paper proposal

55.113 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should permit the inclusion in credit reporting information of the following categories of personal information, in addition to those currently permitted under s 18E of the *Privacy Act*:

- the type of each current credit account opened (for example, mortgage, personal loan, credit card);
- the date on which each current credit account was opened;
- the limit of each current credit account (for example, initial advance, amount of credit approved, approved limit); and
- the date on which each credit account was closed.[162]

55.114 This modest extension of the current reporting system (the ALRC proposal) had some support from both industry and consumer groups. Importantly, credit providers would have access to more information about an individual's current credit commitments to assist in promoting responsible lending. The ALRC stated that this extension in credit reporting information would provide much of the additional predictiveness desired by proponents of more comprehensive reporting.[163]

---

159 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Money Australia, *Submission PR 233,* 12 March 2007; American Express, *Submission PR 257,* 16 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

160 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

161 See, eg, GE Money Australia, *Submission PR 233,* 12 March 2007.

162 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 51–1. These categories of information would replace 'current credit provider' status under *Privacy Act 1988* (Cth) s 18E(1)(b)(v).

163 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [51.165]. The Barron and Staten (2007) research found that an 'intermediate model' between the existing Australian and US credit reporting systems would provide 'some 71% of the reduction in delinquencies achievable under the full US scenario': M Staten and J Barron, *Positive Credit Report Data Improves Loan*

Submissions and consultations

55.115 There was broad support for the implementation of some form of more comprehensive reporting, especially from credit reporting agencies and credit providers.[164] Those in favour of more comprehensive credit reporting included those who supported the ALRC proposal as the preferable model (or as a worthwhile expansion of permissible credit reporting information);[165] and those who favoured further expansion beyond that proposed by the ALRC.[166]

The ALRC proposal

55.116 Dun and Bradstreet submitted that, at this stage, the ALRC proposal 'extends far enough' and finds an 'appropriate balance between the extremes of the existing Australian system and the full-file of the United States':

Decision-Making (2007) Australian Finance Conference, 6. The ALRC's proposed model allows additional categories of credit reporting information to those under the assumed 'intermediate model' and would, therefore, be more rather than less predictive.

164 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; GE Money Australia, *Submission PR 537,* 21 December 2007; Optus, *Submission PR 532,* 21 December 2007; Uniform Consumer Credit Code Management Committee, *Submission PR 520,* 21 December 2007; Confidential, *Submission PR 517,* 21 December 2007; Australian Collectors Association, *Submission PR 505,* 20 December 2007; Veda Advantage, *Submission PR 498,* 20 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; MGIC Australia, *Submission PR 479,* 17 December 2007; HBOS Australia, *Submission PR 475,* 14 December 2007; Westpac, *Submission PR 472,* 14 December 2007; Abacus–Australian Mutuals, *Submission PR 456,* 11 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007; Citibank Pty Ltd, *Submission PR 428,* 7 December 2007; MasterCard Worldwide, *Submission PR 425,* 7 December 2007; Australasian Compliance Institute, *Submission PR 419,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Australian Finance Conference, *Submission PR 398,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007; Confidential, *Submission PR 297,* 1 June 2007; St George Banking Limited, *Submission PR 271,* 29 March 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; AAPT Ltd, *Submission PR 260,* 20 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007.

165 Uniform Consumer Credit Code Management Committee, *Submission PR 520,* 21 December 2007; Confidential, *Submission PR 517,* 21 December 2007; Australian Collectors Association, *Submission PR 505,* 20 December 2007; MGIC Australia, *Submission PR 479,* 17 December 2007; HBOS Australia, *Submission PR 475,* 14 December 2007; ANZ, *Submission PR 467,* 13 December 2007; Abacus–Australian Mutuals, *Submission PR 456,* 11 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007; Australasian Compliance Institute, *Submission PR 419,* 7 December 2007; HSBC, *Submission PR 417,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007.

166 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; GE Money Australia, *Submission PR 537,* 21 December 2007; Veda Advantage, *Submission PR 498,* 20 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; Westpac, *Submission PR 472,* 14 December 2007; ANZ, *Submission PR 467,* 13 December 2007; Abacus–Australian Mutuals, *Submission PR 456,* 11 December 2007; Citibank Pty Ltd, *Submission PR 428,* 7 December 2007; MasterCard Worldwide, *Submission PR 425,* 7 December 2007; Australasian Compliance Institute, *Submission PR 419,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Australian Finance Conference, *Submission PR 398,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

> The ALRC proposal creates a unique opportunity for lenders to demonstrate the benefits that can arise from better quality data and accordingly provides a powerful incentive for lenders to embrace this reform fully.[167]

55.117 While supporting the inclusion of repayment performance information, the ANZ considered that the ALRC proposal constituted 'an appropriately balanced approach that promotes both credit market efficiency and privacy protection'.[168] MGIC Australia stated that

> this small extension will provide credit providers with a more complete knowledge of an individual's current commitments which will assist the lender in applying a prudent approach to credit approval and provide consumers with protection against over-commitment.[169]

55.118 Another group of stakeholders favoured an extension of permissible credit reporting information beyond that proposed by the ALRC. Most submissions from these stakeholders expressly endorsed a model proposed by ARCA. This proposal (the ARCA model), discussed below, would permit credit reporting information to include information about individuals' repayment performance.

55.119 Credit industry stakeholders argued that the additional predictive power that would be available under the ALRC's proposal would be insufficient to justify the expenditure required by credit providers to modify reporting and credit scoring systems to take advantage of the additional data items.[170] The AFC, for example, submitted that

> in order for the industry to participate in a more enhanced reporting environment, there has to be value that off-sets implementation costs. Based on feedback from our members, we submit that … the [ALRC proposal] may have limited value and consequently take-up by the industry. For example, the inclusion of a credit card limit figure does not give a true picture of debtor's commitments unless it can be changed to reflect the balance outstanding at [a] point in time.[171]

55.120 Many stakeholders considered, however, that the addition of repayment performance information would 'tip the balance' and lead to a significant improvement in the ability of credit providers to assess credit worthiness.

The ARCA proposal

55.121 In this context, ARCA proposed that, in addition to the data items comprised in the ALRC proposal,[172] credit reporting information should include a 24-month history of repayment. This would be represented by a series of codes so that the system:

---

167 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007.
168 ANZ, *Submission PR 467,* 13 December 2007.
169 MGIC Australia, *Submission PR 479,* 17 December 2007.
170 Veda Advantage, *Submission PR 498,* 20 December 2007; Westpac, *Submission PR 472,* 14 December 2007; Australian Finance Conference, *Submission PR 398,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.
171 Australian Finance Conference, *Submission PR 398,* 7 December 2007.
172 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 51–1.

> assigns a '0' for no payment required, a '1' for a payment required and made, a '2' for one contractual payments missed, a '3' for two contractual payments missed, and so forth up to '7' for 6 or more payments missed (180 or more days delinquent). Other codes such as 'B' would be recorded if the account was included in a bankruptcy, or 'D' if the status of the account was in 'dispute', or 'H' if the account was involved in a hardship arrangement.[173]

55.122 ARCA considered that this extension to the permitted items proposed by the ALRC would 'significantly improve responsible lending and most importantly will be implemented by credit providers and credit reference agencies'.[174]

55.123 Veda Advantage supported the ARCA approach and stated that it did not believe that 'any further compromise is possible without fatally decreasing the predictive power of the comprehensive information'.[175] Similarly, the ANZ stated that while

> the inclusion of the information proposed by the ALRC will improve marginally the quality of lending decisions and pricing of risk … in order to gain a more accurate and complete assessment of a customer's credit worthiness it is important to have some level of historical repayment data.[176]

Research on predictive value

55.124 The case for allowing credit reporting information to include repayment performance information on the ARCA model was supported by the results of research conducted by several major credit providers following the release of DP 72.

55.125 As discussed in DP 72,[177] Veda Advantage proposed to conduct a data study to model the effect that more comprehensive consumer credit reporting would have on the accuracy of credit providers' application risk evaluation. It proposed to use information from Veda's credit reporting database and more comprehensive 'positive' information, including credit card application, account and payment histories, provided by participating credit providers.[178] This data study did not eventuate, in part because of the constraints imposed by the *Privacy Act*.

55.126 On the initiative of ARCA, and to provide evidence supporting the case for more comprehensive credit reporting, the four major banks and a number of international financial services groups undertook analyses of their own internal data to estimate the relative predictiveness of different variables that might be included in a more comprehensive credit reporting system. The studies assumed a full set of possible

---

173 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.
174 Ibid.
175 Veda Advantage, *Submission PR 498*, 20 December 2007.
176 ANZ, *Submission PR 467*, 13 December 2007.
177 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [51.100].
178 Veda Advantage, *Submission PR 272*, 29 March 2007.

credit reporting variables (including repayment performance information and current balances) to have a 'weighted performance' of 100%, and compared the performance of these comprehensive variables with those permitted by the ALRC and ARCA proposals respectively. The results were reported in the following table:[179]

Table 55–2 Overall weighted contribution to customer behavioural scorecards		
Scenario	Percentage Contribution	Incremental Contribution
Today[180]	10%	10%
ALRC[181]	23%	33%
ALRC + account payment status[182]	22%	55%
ALRC + account payment status + repayment history[183]	19%	74%
Full[184]	26%	100%

55.127 Broadly speaking, the combined result of these studies, by four major banks and a number of international financial services groups, showed that the ALRC proposal would provide 33% of the potential predictive value of fully comprehensive credit reporting.[185] In comparison, the inclusion of repayment performance

179 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

180 This scenario was described as assuming the use of the following data 'current Australian bureau; information on some credit accounts only; extreme negative information only': Ibid.

181 This scenario was described as assuming the use of the following data 'information on all credit accounts; opened date; whether active; limits', including 'consumer or business account; number of account-holders; whether PL is secured or unsecured': Ibid.

182 This scenario was described as assuming the use of the following data 'information on all credit accounts; ALRC information +; delinquency history', including 'consumer or business account; number of days in excess; whether PL is secured or unsecured': Ibid. The ALRC understands that the term 'account payment status' in the table means information about the number of days, if any, account payments are overdue and is, therefore, a subset of 'repayment performance history', as that term is used by the ALRC in this chapter.

183 This scenario was described as assuming the use of the following data 'information on all credit accounts; ALRC information +; delinquency history; repayment history', including 'consumer or business account; number of days in excess; whether PL is secured or unsecured; value, number and dates of repayment': Ibid.

184 This scenario was described as assuming the use of the following data 'current arrangement in the USA (FICO); information on all credit accounts; balance and repayment history; transaction/purchase information; delinquency history', including 'consumer or business account; amount due (credit cards); time and value in excess': Ibid.

185 Ibid.

information, as proposed by ARCA, would provide 74% of the potential predictive value of fully comprehensive credit reporting.[186]

55.128 In assessing the implications of these research results, it should be noted that there are some discrepancies between the assumptions described in the research model and the ALRC and ARCA proposals, as described in DP 72 and in this Report.[187] The research methodology and results have not been independently verified, and the disaggregated results of the research conducted by each institution are commercially sensitive.

55.129 The research results can be viewed from different perspectives. While put forward as evidence of the inadequacy of the ALRC proposal, Dun and Bradstreet commented that the analysis:

> demonstrates that while the greatest benefit comes from a full-file system, there is still considerable benefit from data elements reflecting the ALRC proposed model. In particular it shows that the predictive power arising from adding additional data allowed under the ALRC proposal increases by 23%.[188]

55.130 Some stakeholders suggested that even the ARCA proposal did not go far enough towards a fully comprehensive credit reporting system, which would permit, for example, the inclusion of information about current balances and repayment amounts.[189] In addition, some proponents of the ARCA proposal saw it as a compromise or interim position—and considered that the permitted content of credit reporting information should be expanded further in future.[190]

55.131 ARCA itself noted that 'full comprehensive credit reporting would provide the optimum solution' and has put forward its proposal in order to facilitate a 'gradual process of implementation'.[191] Specifically, credit providers continued to believe that information about current balances should be available through the credit reporting system.[192] National Australia Bank, for example, submitted that

---

186 One of the contributing studies, conducted by Westpac, concluded that the ALRC proposal would provide 38% of the predictive value of comprehensive credit reporting and the ARCA model would provide 60% of the potential predictive value: Westpac, *Submission PR 472,* 14 December 2007.

187 For example, the ALRC proposal, as described in DP 72, would also permit the use of information about closed accounts: Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 51–1. The ARCA proposal, as described in ARCA's submission, would not permit the use of the values of repayments: Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

188 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007.

189 GE Money Australia, *Submission PR 537,* 21 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; MasterCard Worldwide, *Submission PR 425,* 7 December 2007.

190 Citibank Pty Ltd, *Submission PR 428,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

191 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

192 See, eg, GE Money Australia, *Submission PR 537,* 21 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; Citibank Pty Ltd, *Submission PR 428,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

> the balance of credit account and/or associated limit utilisation would provide for an even more informed lending decision to ensure borrowers are not placed in situations where they cannot meet their obligations. This should be considered as a future enhancement.[193]

55.132 Citibank Pty Ltd maintained the view that including the current outstanding balance should be permitted 'to provide the optimum support for responsible lending and assessing customers credit worthiness'.[194] MasterCard stated:

> Without allowing current balance information to be stored on an individual's credit report, lenders do not have a source to confirm whether the statement is an accurate reflection of the borrower's true position.[195]

Opposition to more comprehensive credit reporting

55.133 Consumer groups, privacy advocates and regulators generally opposed more comprehensive credit reporting.[196] The potential benefits of, and some of the problems associated with, more comprehensive reporting as perceived by these stakeholders are discussed above. These stakeholders also focused on alternatives, and desirable pre-conditions to, the possible introduction of more comprehensive credit reporting.

55.134 Some stakeholders observed that, if additional information is required by credit providers in order to assess an individual's eligibility for credit, this information can be sought from the individual directly or from a third party with the individual's consent.[197]

55.135 The Banking and Financial Services Ombudsman (BFSO) noted that credit providers can reduce information asymmetry 'by asking for details of all current credit facilities as part of the application process and requiring consumer declarations as to the accuracy of the information'. Therefore, addressing the 'absence of a comprehensive dispute resolution regime and the ability to report unregulated credit … would appear to be the more immediate priorities' than implementing more comprehensive credit reporting.[198] Telstra stated that the additional information

---

193 National Australia Bank, *Submission PR 408,* 7 December 2007.

194 Citibank Pty Ltd, *Submission PR 428,* 7 December 2007.

195 MasterCard Worldwide, *Submission PR 425,* 7 December 2007.

196 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; National Legal Aid, *Submission PR 521,* 21 December 2007; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Galexia Pty Ltd, *Submission PR 465,* 13 December 2007; Telstra Corporation Limited, *Submission PR 459,* 11 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

197 Telstra Corporation Limited, *Submission PR 459,* 11 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

198 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007. The Consumer Action Law Centre also considered that improved complaint-handling and enforcement mechanisms

proposed to be permitted by the ALRC is available to credit providers who 'wish to make the relevant inquiries and obtain the required consents' and 'should not automatically form part of credit information files'.[199]

55.136 Some stakeholders who opposed the introduction of more comprehensive credit reporting submitted that the focus of the present Inquiry should be on reforms to improve the current credit reporting system, before any consideration is given to its extension. In this context, the Victorian Review noted that alternatives to both the status quo and comprehensive credit reporting include:

- Improving the existing negative reporting scheme in terms of its accuracy.
- Providing additional incentives for credit reporting agencies to maintain accurate and complete data. For example, requiring credit reporting agencies to pay a specified amount to a consumer in each case where information is reported as inaccurate may assist in addressing current information asymmetry within the current system.
- Requiring consumer declarations in relation to loan applications.
- Expanding financial literacy programs to encourage better self-selection by consumers and shopping for credit by consumers.[200]

55.137 The Australian Privacy Foundation submitted that the ALRC should recommend that any further consideration of comprehensive reporting be 'deferred until after experience with an initial round of reforms resulting from the current Review'.[201] National Legal Aid also stated that it would oppose the introduction of more comprehensive reporting 'until there is positive progress on addressing the major defects of the current scheme'.[202]

55.138 A number of stakeholders suggested that further study is required before reaching any decision to recommend the implementation of more comprehensive credit reporting,[203] including studies which focus on the possible impact on over-indebtedness and access to affordable credit.[204]

55.139 The OPC submitted that independent research should be conducted on the impact that comprehensive credit reporting would have on the Australian financial system and Australian consumers. It was suggested that this research should provide

---

should be more of a priority than the possible introduction of more comprehensive reporting: Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

199 Telstra Corporation Limited, *Submission PR 459,* 11 December 2007.

200 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 272.

201 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

202 National Legal Aid, *Submission PR 265,* 23 March 2007.

203 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

204 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

recommendations about: whether comprehensive credit reporting should be introduced in Australia; and, if comprehensive credit reporting were to be introduced, what model should be adopted; which industry participants should be included in the expanded system; and what compliance framework should be imposed. The ALRC's proposals would be considered as part of this research.[205]

Credit reporting and responsible lending

55.140 The link between more comprehensive reporting and responsible lending practices was highlighted by consumer and privacy advocates. These stakeholders considered that changes to consumer credit regulation to require responsible lending should be a pre-condition to the introduction of more comprehensive credit reporting.[206] The Consumer Action Law Centre, for example, stated:

> Appropriate regulation of credit marketing and irresponsible lending in Australia could minimise the negative effects of expanding credit reporting information. However this would need to be implemented before consideration is given to expanding credit reporting information.[207]

55.141 The Cyberspace Law and Policy Centre submitted that:

> No additional classes of information should be permitted in credit information files unless there are simultaneous changes to consumer credit regulation including an obligation to lend responsibly including taking into account all available information.[208]

55.142 It was observed that while industry stakeholders, in promoting a move towards more comprehensive credit reporting, have emphasised potential benefits in relation to responsible lending, credit providers are under no positive legal obligation to engage in responsible lending. Galexia noted that the limited 'shield' provision of the *Consumer Credit Code*[209] (discussed above) under which a court may reopen an unjust transaction is the only relevant legislative provision.[210]

> There is no general licensing scheme or regulation for credit providers in Australia that requires them to be responsible lenders. Specifically there is no requirement that lenders assess a consumers' ability to repay a loan without suffering undue hardship.[211]

---

205 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.

206 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; National Legal Aid, *Submission PR 521,* 21 December 2007; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

207 Consumer Action Law Centre, *Submission PR 510,* 21 December 2007.

208 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

209 *Consumer Credit Code* s 70(1).

210 Galexia stated that 'this provision has proved to be difficult to use in practice'. The provision 'does not require any proactive steps by credit providers and it usually involves considerable time, expense and legal representation to re-open a credit contract on the grounds that it is unjust': Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

211 Ibid.

ALRC's view

55.143 The ALRC recognises that, according to widely accepted economic theory, making more information available to credit providers will tend to increase efficiency in the market for credit. It also will assist in making credit more available to those able to repay and reduce rates of default (or both).[212] There was no significant disagreement among stakeholders that more comprehensive credit reporting has the potential to improve risk assessment by credit providers, even among those who expressed concerns about how this improved risk assessment would be used in the credit market.

55.144 There are many possible approaches to reform of the credit reporting provisions to permit more comprehensive credit reporting. The spectrum of choice ranges from recommending no changes in the categories of information now permitted, extensions to these categories such as those as proposed by the ALRC in DP 72 and by ARCA, through to fully comprehensive credit reporting such as exists in the US.

Benefits of more comprehensive credit reporting

55.145 Proponents of more comprehensive credit reporting have sought to justify reform by reference to potential benefits arising from improved credit market competition and efficiency, resulting in decreased levels of consumer over-indebtedness and default, lower cost and higher availability of credit.

55.146 While industry stakeholders have presented considerable evidence and argument to support these expected outcomes, the ALRC is not convinced these outcomes are sufficiently certain to justify the implementation of more comprehensive credit reporting. The fundamental point is that any credit reporting system is only one tool, albeit an important one, used by credit providers to assess risk and to determine lending practices. This tool can be used in different ways, which may depend on other factors including, for example, a particular credit provider's competitive position in the market. The information available through the credit reporting system ultimately cannot dictate what lending practices will emerge or prevail in the marketplace.

55.147 This fact has been emphasised recently by the so-called 'subprime' crisis. In the US, high levels of default on subprime loans contributed to an ongoing liquidity crisis in global financial markets, which began in mid-2007.[213] While the term 'subprime' is not consistently defined in the marketplace or among individual institutions, US regulators have defined subprime lending as

---

212 See, eg, the literature reviews in J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 5 May 2008.

213 For example, a range of factors relating to the operation of markets dealing with collateralised debt obligations were also important in the development of the liquidity crisis.

> programs that target borrowers with weakened credit histories typically characterized by payment delinquencies, previous charge-offs, judgments, or bankruptcies. Such programs may also target borrowers with questionable repayment capacity evidenced by low credit scores or high debt-burden ratios.[214]

55.148 The comprehensive credit reporting information available to lenders in the US might be expected to have assisted lenders in proper risk assessment. Commentary has suggested, however, that credit scoring such as that provided by the Fair Isaac Corporation (FICO) was not effective in preventing lenders from advancing risky loans:

> FICO scores are built on data gathered by the three big credit bureaus. The score is heavily influenced by the amount of debt a borrower already has and by payment history … But mortgage lenders got a little too confident in FICO and failed to give adequate weight to two other factors in a mortgage application: how much the borrower is putting down and how well he has documented his income.[215]

55.149 The ALRC recognises that risk assessment practices were not the only factor contributing to the subprime crisis. Other factors included aggressive marketing practices, such as the use of low fixed introductory ('teaser') interest rates, and promoting loans through brokers with financial incentives to close deals.[216] Arguably, one lesson that may be drawn from the US subprime lending experience is that the availability of comprehensive credit reporting information, on which to base proper risk assessment, will not necessarily produce responsible lending. The availability of risk assessment tools do not dictate lending policies—lenders do.

55.150 Some stakeholders identified the current Australian economic environment as an important reason to implement more comprehensive reporting.[217] Veda Advantage, for example, referred to high levels of household debt and concerns about an economic downturn and stated that:

> In these circumstances, Australian borrowers and lenders need the best credit information and stronger consumer protection to help manage their risk. This is the most compelling argument for reform of the credit reporting provisions of the *Privacy Act*.[218]

---

214 Federal Deposit Insurance Corporation, *Examination Guidance for Subprime Lending Programs* (2001) <www.fdic.gov/news/news/financial/2001/fil0109.html> at 5 May 2008; United States Department of the Treasury, Federal Deposit Insurance Corporation and National Credit Union Administration, *Statement on Subprime Mortgage Lending* (2007) Federal Reserve <www.federalreserve.gov/newsevents/press/bcreg/bcreg20070629a1.pdf> at 26 November 2007.

215 M Maiello, 'Where was FICO?: The Widespread Use of No-Money-Down Mortgages Flummoxed the Best-Known Scorer of Creditworthiness', *Forbes Online*, 17 September 2007, <members.forbes.com/forbes/2007/0917/044.html>.

216 J Vigdor, *What Should Government Do About the Subprime Mortgage Market?: A Taxpayer's Guide* (2007) National Taxpayers Union.

217 GE Money Australia, *Submission PR 537,* 21 December 2007; Veda Advantage, *Submission PR 498,* 20 December 2007.

218 Veda Advantage, *Submission PR 498,* 20 December 2007.

55.151 As discussed above, it is hard to draw any firm conclusions about the impact of credit reporting systems on credit markets and the economy generally. In any case, research results cannot determine the policy position to be adopted. Any proven economic benefit still needs to be balanced against individual privacy rights and the risk of breach of those rights. An appropriate balance needs to be struck between efficiency in credit markets and privacy protection.

55.152 The most compelling argument for more comprehensive credit reporting is based on assisting credit providers to practise responsible lending. More comprehensive credit reporting clearly has the potential to enable credit providers to assess better individuals' capacity repay and the risk that credit will not be repaid.

55.153 The current limitations on the permitted content of credit reporting information do not work in the best interests of either industry or consumers. As noted above, industry research suggests that the credit reporting information currently available provides only 10% of the potential predictive value of fully comprehensive credit reporting.[219] Whatever the precision of this figure, it is clear that the existing constraints significantly limit the predictive power of credit reporting information.

55.154 An effective credit reporting system should enable a credit provider to verify an individual's potential credit commitments. The additional categories of credit reporting information recommended by the ALRC would assist to highlight discrepancies with the information provided by an individual credit applicant. At the very least, credit providers should be able to confirm whether an inquiry from another credit provider resulted in credit being granted. From the consumer side, there are also concerns about the currently misleading nature of inquiry information.[220]

Repayment performance information

55.155 The categories of personal information currently permitted in credit reporting information should be augmented, as proposed in DP 72.[221] The remaining question is whether the categories should be extended further to include repayment performance information, along the lines suggested by ARCA and others. A good case for the inclusion of repayment performance information can be made.

55.156 ARCA has proposed that credit reporting information should include a 24-month history of repayment.[222] This would not record the amount of any repayment, but would represent repayments by codes indicating, at each point in the repayment

219 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.
220 See Ch 56.
221 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 51–1.
222 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

cycle, whether a repayment was required and whether contractual payments have been missed.[223]

55.157 At present, the *Privacy Act* permits the inclusion in credit information files of information about credit where the individual is at least 60 days overdue in making a payment and the credit provider has taken steps towards recovery of the amount outstanding.[224] This is often referred to as 'default' information or overdue payment information.

55.158 From one perspective, the proposed 'negative' repayment performance information is simply a more differentiated and comprehensive version of the default information currently collected—relevant to more specific time periods and forming a historical record. Under the ARCA proposal, the system also would record that no repayment was required or that a repayment was required and made. This information is 'positive' information that tends to work in favour of an individual in his or her dealings with credit providers, by indicating willingness to repay.

55.159 Some credit providers and credit reporting agencies suggest that the more limited extension of the credit reporting system proposed by the ALRC may not provide a sufficient incentive for the industry to bear the costs of implementation—despite, on ARCA's figures, contributing another 23% of the predictive power of the full set of credit reporting variables. This view was not shared by other industry stakeholders, as discussed above, and is not accepted by the ALRC. Credit providers have, nevertheless, presented a strong case that repayment performance information would significantly improve the predictive value of credit reporting information and would be implemented by credit providers, if permitted by law.

55.160 The ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include some repayment performance history. For these purposes, an individual's repayment performance history should comprise only information indicating:

- whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not

- the number of repayment cycles the individual was in arrears.

55.161 The ALRC recognises that implementation of this recommendation will result in the sharing between credit reporting agencies and credit providers of more detailed information about the conduct of individuals with respect to credit and, therefore, a corresponding reduction in information privacy.

---

223 Ibid.

224 *Privacy Act 1988* (Cth) s 18E(1)(b)(vi). The ALRC understands that, in practice, credit providers do not usually report overdue payment information until at least 90 days after default.

55.162 Credit reporting agencies will be permitted, for example, to collect and report information indicating that an individual was on time, or 30, 60 or 90 days late, in making a payment due under his or her credit card or other credit account. This detailed information may be collected about any individual who opens a credit account, even where that individual has never failed to meet his or her credit obligations. The information, as is the case with existing credit reporting information, will be collected, used and disclosed without the express consent of the individual concerned.

55.163 The recommended system of more comprehensive credit reporting would, however, retain the prohibition on the collection or reporting of the current balances of credit accounts or the amounts of repayments made or overdue.

55.164 For the reasons set out in this chapter, the ALRC concludes that the balance tips in favour of allowing repayment performance information provided that, as discussed below, consideration is given to the enactment of new responsible lending obligations.

55.165 Further, the ALRC's recommendations that an extension be permitted in the categories of personal information that may be collected in credit reporting are intended as part of broader reform of the credit reporting system. Submissions emphasised the need to review and improve the existing regime of privacy protection, regardless of whether more comprehensive credit reporting is permitted by legislation or implemented by the finance industry.[225]

55.166 The ALRC agrees with this approach. Other changes to the regulation of credit reporting recommended in Chapters 56–59 are intended, among other things, expressly to prohibit the use or disclosure of credit reporting information in direct marketing, promote consistency and accuracy in the reporting of overdue payments, and improve complaint-handling and dispute resolution processes. If these other changes are not implemented, the foundation to support more comprehensive credit reporting falls away.

Responsible lending obligations

55.167 In the course of the Inquiry, it became clear that many stakeholders considered that consumer credit legislation should be reformed to promote more responsible lending before any form of more comprehensive credit reporting is introduced. Galexia, for example, stated that regulation of responsible lending and credit marketing should include regulation of 'what factors should be included in a proper assessment of a consumer's capacity to repay a loan'.[226]

---

225 See, eg, N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.
226 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

55.168 A number of parliamentary reports have recommended reform relevant to responsible lending obligations. In 2005, the Senate Economics Committee recommended that the states and the Northern Territory develop 'uniform consumer credit legislation requiring credit providers to undertake appropriate checks of borrowers' capacity to pay before issuing new credit cards or raising credit limits'.[227]

55.169 In its 2007 report *Home Loan Lending*,[228] the House of Representatives Standing Committee on Economics, Finance and Public Administration outlined a range of concerns with the current *Consumer Credit Code* regime, including the weak requirements on credit providers to assess individuals' capacity to repay and the ability of credit providers to avoid the *Consumer Credit Code* by requiring individuals to sign 'business purpose declarations'.[229] The Committee concluded that credit regulation 'has failed to keep pace with the rapidly evolving and growing credit market' and is 'ineffective in dealing with the new practices that have emerged'.[230] The Committee recommended that, in future, the Australian Government should regulate credit products and advice, including regulation of mortgage brokers and non-bank lenders.[231]

55.170 The states and territories have sought generally to maintain harmonisation of consumer credit law through the uniform *Consumer Credit Code*. Issues concerning responsible lending are included on the current Strategic Agenda[232] of the Ministerial Council on Consumer Affairs.[233]

55.171 In addition, Australia's consumer policy framework (including the *Consumer Credit Code*) is subject to a current review by the Productivity Commission. In its draft report, released in December 2007, the Productivity Commission made a draft recommendation that responsibility for regulating finance brokers and other credit

---

227 Parliament of Australia—Senate Economics Committee, *Consenting Adults, Deficits and Household Debt—Links Between Australia's Current Account Deficit, the Demand for Imported Goods and Household Debt* (2005), rec 7. The Committee stated that the *Fair Trading Act* 1992 (ACT) provided an appropriate model.

228 Parliament of Australia—House of Representatives Standing Committee on Economics Finance and Public Administration, *Home Loan Lending: Inquiry into Home Loan Lending Practices and the Processes Used to Deal with People in Financial Difficulty* (2007).

229 Ibid, 43. The *Consumer Credit Code* makes a distinction between credit 'provided or intended to be provided wholly or predominantly for personal, domestic or household purposes', which is regulated by the Code, and other credit, which is not: *Consumer Credit Code* s 6(1)(b).

230 Parliament of Australia—House of Representatives Standing Committee on Economics Finance and Public Administration, *Home Loan Lending: Inquiry into Home Loan Lending Practices and the Processes Used to Deal with People in Financial Difficulty* (2007), 49.

231 Ibid, rec 2. Galexia noted that an exposure draft *Finance Broking Bill 2007* (NSW), prepared by the Ministerial Council on Consumers Affairs, and intended as uniform national legislation, contains provisions requiring finance brokers to take proactive steps to assess a consumer's ability to repay: Galexia Pty Ltd, *Submission PR 465,* 13 December 2007. See Ministerial Council on Consumer Affairs, *National Finance Broking Scheme Consultation Package* (2007), exposure draft *Finance Broking Bill 2007* (NSW) cl 33(3)–(4).

232 Ministerial Council on Consumer Affairs, *Ministerial Council on Consumer Affairs: Strategic Agenda* (2007) <www.consumer.gov.au/html/mcca_projects.htm> at 5 May 2008.

233 The Ministerial Council on Consumer Affairs consists of all Commonwealth, state, territory and New Zealand ministers responsible for fair trading, consumer protection laws and credit laws.

providers should be transferred to the Australian Government, with the regulatory requirements encompassed within the regime for financial services administered by the Australian Securities and Investments Commission. As part of this transfer, the Productivity Commission suggested that the *Consumer Credit Code* and related credit regulation, appropriately modified, should be retained and that federal, state and territory governments 'should give priority to determining the precise requirements, and how they would be best incorporated within the broader regime'.[234]

55.172 As observed by Veda Advantage, industry and consumer stakeholders often 'contextualise' discussion of credit reporting regulation by reference to concerns about responsible lending and consumer credit regulation more generally.[235] The UCCCMC observed that the existence of more comprehensive reporting is 'relevant to any decision about the feasibility of imposing a statutory requirement on lenders to assess capacity to repay'.[236]

55.173 On the other hand, industry has expressed the view that privacy law (including reform of the credit reporting provisions) should not be used as a 'proxy measure to mitigate consumer harms that are more properly dealt with in other jurisdictions'[237] or as a 'vehicle for indirectly regulating consumer lending'.[238]

> The better view is that if, as a matter of policy, the government determines that additional obligations with respect to responsible lending should be imposed on credit providers, those obligations should be imposed directly through the consumer credit laws.[239]

55.174 Assisting credit providers to practise responsible lending is the most compelling argument for more comprehensive credit reporting. Some have questioned, however, whether more responsible lending will be an outcome of introducing comprehensive credit reporting, in the absence of new legislative obligations on credit providers.[240]

55.175 In the ALRC's view, it would be inappropriate for this Inquiry to recommend specific changes to the *Consumer Credit Code* or other consumer credit legislation. Legislation relating to responsible lending is not referred to expressly in the Terms of Reference of the Inquiry—although, as is standard, the Terms of Reference direct the

---

234 Productivity Commission, *Draft Report: Review of Australia's Consumer Policy Framework* (2007), 65, draft rec 5.2.

235 Veda Advantage, *Submission PR 498,* 20 December 2007.

236 Uniform Consumer Credit Code Management Committee, *Submission PR 520,* 21 December 2007.

237 Veda Advantage, *Submission PR 498,* 20 December 2007.

238 GE Money Australia, *Submission PR 537,* 21 December 2007.

239 Ibid.

240 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; National Legal Aid, *Submission PR 521,* 21 December 2007; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

ALRC to consider 'any related matter'. More importantly, specific changes to consumer credit legislation were not a focus of detailed consultation during the course of the Inquiry.

55.176 As discussed above, however, the ALRC established that there is a clear link between this issue and the possible implementation of more comprehensive credit reporting. The additional categories of personal information to be included in credit reporting information recommended in Recommendation 55–1 can be seen as an incremental extension of existing permitted content. Permitting the inclusion of repayment performance history, however, would be a more significant change.

55.177 The ALRC recommends, therefore, that repayment performance history only should be permitted to be contained in credit reporting information if the Australian Government is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation. In making this assessment reference could be made to the Productivity Commission's report on Australia's consumer policy framework, this ALRC Report, and any future review of the *Consumer Credit Code*.

Regulating for permitted content

55.178 In Chapter 56, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information. This list should be based on the provisions of s 18E of the *Privacy Act*, subject to the changes set out in Recommendations 55–1, 55–2, 56–2 to 56–4, 56–6, 55–8 and 55–9.

55.179 Periodic review of the regulations would provide adequate flexibility for industry, while protecting the privacy of individuals. Given the relative resources of industry and consumer stakeholders, any further reduction in privacy caused by expanding the permitted content of credit reporting information should be subject to parliamentary scrutiny and consultation with consumer groups, privacy advocates and the regulator.

55.180 It would be appropriate, however, for detail on how repayment performance history is to be recorded to be set out in the credit reporting code. As discussed in Chapter 54, the ALRC recommends that credit reporting agencies and credit providers should develop, in consultation with consumer groups and regulators, including the OPC, a credit reporting code providing detailed guidance within the framework provided by the regulations.[241] The credit reporting code should deal with a range of operational matters, including procedures for the reporting of repayment performance history.

---

241 See Rec 54–9.

Permissible retention periods

55.181 Part IIIA of the *Privacy Act* contains detailed provisions requiring credit reporting agencies to ensure that personal information contained in credit information files is deleted after the expiry of prescribed maximum permissible periods.[242] As discussed in Chapter 58, the ALRC concludes that there is no compelling case for any major change to the existing retention periods and recommends that the regulations should provide for the deletion of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently applying.

55.182 A new retention period, however, needs to be set for new permitted content of credit reporting information—that is, information about open credit accounts and their current limits, and credit accounts that have been closed. No new retention period needs to be set for repayment performance information, because the new *Privacy (Credit Reporting Information) Regulations* should provide that only information relating to an individual's credit over the prior two years is to be included. The ALRC recommends that the regulations provide for the deletion of credit account information two years after the date on which a credit account is closed. This would ensure that repayment performance information about accounts that have been closed is retained for no longer than that relating to current credit accounts.

Recommendation 55–1 The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include the following categories of personal information, in addition to those currently permitted in credit information files under the *Privacy Act*:

(a) the type of each credit account opened (for example, mortgage, personal loan, credit card);

(b) the date on which each credit account was opened;

(c) the current limit of each open credit account; and

(d) the date on which each credit account was closed.

Recommendation 55–2 Subject to Recommendation 55–3, the new *Privacy (Credit Reporting Information) Regulations* should also permit credit reporting information to include an individual's repayment performance history, comprised of information indicating:

242 *Privacy Act 1988* (Cth) s 18F.

(a) whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not,

(b) the number of repayment cycles the individual was in arrears.

Recommendation 55–3 The Australian Government should implement Recommendation 55–2 only after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

Recommendation 55–4 The credit reporting code should set out procedures for reporting repayment performance history, within the parameters prescribed by the new *Privacy (Credit Reporting Information) Regulations*.

Recommendation 55–5 The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of the information referred to in Recommendation 55–1 two years after the date on which a credit account is closed.

Other aspects of the model

55.183 Stakeholders have raised a number of other matters relevant to a move towards more comprehensive credit reporting. For example, concerns were expressed that, if credit reporting information is to include information about credit accounts that have been closed (as recommended above), regulation needs to include a definition of a 'closed account' since there is 'no general industry practice'.[243] The OPC suggested, in this context, that a credit provider should be required to notify the credit reporting agency, as soon as practicable, that the account has been closed.[244]

55.184 Legal Aid Queensland expressed concern about the timeliness of repayment performance information, especially given its view that the industry struggles to list existing default information in a timely manner under the current regime and that reporting repayment performance information would make it easier for credit providers and debt collectors to 'use the credit reporting system as a means of pressuring borrowers to repay accounts when there is a question as to liability'.[245]

243 Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

244 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.

245 Legal Aid Queensland, *Submission PR 489,* 19 December 2007.

55.185 The ALRC makes no recommendation with regard to these issues, but observes that they may be appropriate subjects for consideration as part of developing a credit reporting industry code (see Recommendation 54–10).

55.186 In addition, some stakeholders considered that, if Australian law is amended to permit more comprehensive credit reporting, the sharing of this information between credit providers should operate in accordance with the principle of reciprocity. This issue is discussed below.

Reciprocity and compulsory reporting

55.187 In relation to data sharing among credit providers, the principle of reciprocity has been expressed as dictating that 'data will be shared on the principle that subscribers receive the same credit performance level data that they contribute, and should contribute all such data available'.[246]

55.188 One of the stated aims of ARCA is to improve data standards and consistency, including by promoting the principle of reciprocity.[247] The UK provides one model in this regard. In the UK, the finance industry established the Steering Committee on Reciprocity to develop guidelines on the 'use and sharing of credit performance and related data on individuals'. This body consists of representatives from credit providers and credit reference agencies and has produced principles of reciprocity that set out the 'rules for the recording, supply and access of credit performance data' shared through the credit reporting agencies.[248]

55.189 The principle of reciprocity is closely related to the concept of compulsory reporting—the idea that it should be compulsory for credit providers to report some or all kinds of credit reporting information. The value of credit reporting information may be reduced significantly by the fact that credit providers may 'pick and choose' whether information about particular overdue payments or other adverse information is reported. On the other hand, compulsory reporting obligations may interfere with the relationship between a credit provider and its customers—for example, when negotiating a repayment plan with an overcommitted individual.

55.190 Some credit providers supported compulsory reporting as desirable, but not necessarily as a subject appropriate for regulation.[249] Others opposed compulsory reporting because of possible compliance costs for smaller credit providers[250] and

246 Steering Committee on Reciprocity, *Information Sharing: Principles of Reciprocity* (2003), 3.
247 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.
248 Steering Committee on Reciprocity, *Information Sharing: Principles of Reciprocity* (2003).
249 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Westpac, *Submission PR 256,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007; National Credit Union Association Inc, *Submission PR 226,* 9 March 2007.
250 Min-it Software, *Submission PR 236,* 13 March 2007.

telecommunications service providers.[251] In addition, some stakeholders noted that compulsory reporting of default information could prevent negotiated settlements[252] and, by removing discretion in reporting, diminish the effectiveness of important provisions of the *Code of Banking Practice*, which requires a subscribing bank to try to help customers overcome difficulties with credit.[253]

55.191 Another related concept is that of 'tiered' access to credit reporting information, including access for non-credit related purposes, such as debt collection and identity verification. Tiered access can be based on reciprocity, or take other factors into account so that subscribers may obtain some categories of information that they do not provide to the agency. For example, some companies might be permitted to use credit reporting information for identity verification, despite not providing information on their own customers.[254]

55.192 In DP 72, the ALRC noted that credit providers generally support the principle of reciprocity in credit reporting and obligations consistently to report information.[255] Support was not universal, however, and some participants in the existing credit reporting system stated that contributing data to a more comprehensive system should not be compulsory.[256]

55.193 In DP 72, the ALRC concluded that credit providers themselves and their industry associations should take responsibility for deciding how information sharing should proceed within the framework provided by legislation. It would not, therefore, be appropriate for the new regulations to mandate reporting obligations. The ALRC proposed, nevertheless, that the credit reporting industry code should provide for access according to principles of reciprocity.[257]

55.194 This proposal was generally supported,[258] but subject to many qualifications and exceptions. Stakeholders highlighted the complexity of applying reciprocity

---

251 Optus, *Submission PR 258,* 16 March 2007.

252 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

253 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007. Optus made a similar point in relation to the *Telecommunications Credit Management Code of Practice*: Optus, *Submission PR 258,* 16 March 2007.

254 Veda Advantage, *Submission PR 272,* 29 March 2007.

255 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [51.132].

256 AAPT Ltd, *Submission PR 260,* 20 March 2007; Optus, *Submission PR 258,* 16 March 2007.

257 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 51–2.

258 GE Money Australia, *Submission PR 537,* 21 December 2007; Veda Advantage, *Submission PR 498,* 20 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; HBOS Australia, *Submission PR 475,* 14 December 2007; ANZ, *Submission PR 467,* 13 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Australian Finance Conference, *Submission PR 398,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344,* 19 November 2007. Galexia stated that 'in light of the cost and complexity of developing an industry Code, some further consideration should be given to including reciprocity and data consistency in the Regulations': Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

principles.[259] ARCA stated that the practical implementation of reciprocity is likely to be 'more complex' than suggested in DP 72:

> To illustrate: as credit providers are from different industries, ARCA believes that a credit provider shares all available information from its particular industry eg a Telco should be able to access all credit reporting information from a different industry eg a bank. ARCA also acknowledges that although there may be limitless variations to the forms of reciprocity, it may for implementation purposes also need to keep the policy relatively simple. As this is only of relevance to industry it is recommended that this is the responsibility of the industry [code of conduct] to manage.[260]

55.195 ARCA also referred to the need for flexibility during the implementation period, so that reciprocity is able to be phased in according to the reporting and other capabilities of credit providers.[261] Similarly, Veda Advantage stated that it supported a system of tiered access 'whereby [credit reporting agencies] can assess a subscriber's access to information based on their capacity to meet compliance requirements and the extent of risk they face'.[262]

55.196 GE Money provided detailed views on how principles of reciprocity should be implemented to distinguish between existing and more comprehensive categories of credit reporting information. GE Money submitted that telecommunications companies, for example, should be able to elect to provide and receive only the existing 'negative' default information, but not more comprehensive repayment performance information.[263]

55.197 Legal Aid Queensland expressed concern that reciprocity, by requiring all defaults to be reported, would reduce the incentive for consumers and credit providers to negotiate settlements of debts. Further,

> There is no evidence from industry, even with the inclusion of better data accuracy and the availability of more comprehensive information, that data scoring will allow those consumers with one default to access mainstream credit. Consequently, if reciprocity is required in relation to credit reporting of negative information, it may in our view result in more consumers accessing fringe credit.[264]

---

259 Legal Aid Queensland, *Submission PR 489,* 19 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

260 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007.

261 Ibid.

262 Veda Advantage, *Submission PR 498,* 20 December 2007.

263 GE Money Australia, *Submission PR 537,* 21 December 2007.

264 Legal Aid Queensland, *Submission PR 489,* 19 December 2007.

55.198 The Insurance Council of Australia submitted that it would be inappropriate to apply principles of reciprocity in credit reporting to mortgage insurers.[265] Telstra also expressed a range of concerns about reciprocity, which, it stated, may lead to 'unnecessary disclosure and inflexibility' and constitute an unnecessary burden on credit providers:

> Credit providers require discretion to assess whether disclosure is appropriate in each borrower's circumstances. They should not be penalised for having and using such discretions sensibly by being denied access to credit reporting. This could ultimately harm the individuals whose personal information is intended to be protected.[266]

55.199 Some stakeholders stated that the ALRC should not take a position on reciprocity at this stage.[267] The Cyberspace Law and Policy Centre submitted that reciprocity 'is largely a commercial issue for the industry stakeholders', and any agreement would be likely to require Australian Competition and Consumer Commission authorisation under the *Trade Practices Act 1974* (Cth). Therefore, the ALRC should not take a position on 'whether participation in a centralised credit reporting system should be based on a principle of reciprocity'.[268]

55.200 The OPC supported the view that credit providers and credit reporting agencies should have responsibility for determining how access to credit reporting information is to be managed, and suggested that further research into comprehensive credit reporting include consideration of principles of reciprocity.[269] The Australian Privacy Foundation stated that the ALRC should remain neutral on the issue of reciprocity and should instead 'endorse principles of tiered access and separate justification for input to and output from credit reference databases'.[270]

ALRC's view

55.201 Most stakeholders agreed that, in order for more comprehensive credit reporting to benefit the operation of the credit market, reporting by credit providers of the additional data items needs to be as universal as possible. Reporting according to principles of reciprocity may be an important mechanism by which to achieve this aim.

55.202 Beyond the general proposition that, in general, credit providers only should have access to the same categories of personal information that they provide to the credit reporting agency, there lies considerable complexity. Credit providers come from different industries and have different data requirements and capacities to provide data to the credit reporting system. The relative costs and benefits of participation in the credit reporting system differ between classes of credit provider, which may raise

---

265 Insurance Council of Australia, *Submission PR 485,* 18 December 2007.
266 Telstra Corporation Limited, *Submission PR 459,* 11 December 2007.
267 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.
268 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.
269 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.
270 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

competition issues. For these reasons, issues concerning reciprocity, tiered access and compulsory reporting are matters that should be resolved by credit providers and their industry associations, in consultation with consumer groups and regulators, within the framework set by regulation. Once resolved, these matters may be appropriate for inclusion in the credit reporting industry code.

56. Collection and Permitted Content of Credit Reporting Information

Contents

Introduction

56.1 This chapter discusses the existing provisions of Part IIIA of the *Privacy Act 1988* (Cth) dealing with the collection (and notification of collection) of information in credit information files and credit reports. Recommendations are made on how these matters should be dealt with under the Unified Privacy Principles (UPPs)[1] and the new *Privacy (Credit Reporting Information) Regulations*.

56.2 The issues in this chapter and Chapters 57–58 are discussed broadly in the order the privacy principles are set out in the model UPPs. Where applicable, the provisions of the UPPs and Part IIIA of the *Privacy Act* are compared briefly.

1 See Part D.

Collection and notification

56.3 The 'Collection' principle in the model UPPs provides that an agency or organisation may only collect personal information:

- that is necessary for one or more of its functions or activities;
- by lawful and fair means and not in an unreasonably intrusive way; and
- about an individual from that individual, if it is reasonable and practicable to do so.

56.4 The 'Notification' principle provides that, at or before the time an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take steps to notify the individual, or ensure that the individual is aware of, the:

- fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;
- identity and contact details of the agency or organisation;
- rights of access to, and correction of, personal information provided by the UPPs;
- purposes for which the information is collected;
- main consequences of not providing the information;
- actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information;
- fact that the avenues of complaint available to the individual are set out in the agency's or organisation's Privacy Policy; and
- fact, where applicable, that the collection is required or authorised by or under law.

56.5 The provisions of Part IIIA of the *Privacy Act* depart significantly from these principles (and the equivalent NPP) in two relevant respects. First, s 18E of the *Privacy Act* sets out exhaustively the permitted content of credit information files held by credit reporting agencies.[2] No other personal information may be included in an individual's credit information files, even if the information is 'necessary' in terms of the privacy principles.

---

2 The permitted content of credit information files is summarised in Ch 53.

56.6 Secondly, Part IIIA contains a specific notification obligation in that, under s 18E(8)(c), a credit provider must not give personal information relating to an individual to a credit reporting agency if 'the credit provider did not, at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a credit reporting agency'.

56.7 Issues relating to the permitted content of credit reporting information and notification of the collection of credit reporting information are discussed below.

Permitted content of credit reporting information

56.8 There was no call for removing regulation dealing specifically with the permitted content of credit reporting information and leaving the matter to be governed by the model UPPs. Any such move would create uncertainty about the scope of information that may be 'necessary' to assess credit risk or for other functions or activities of credit reporting agencies or credit providers. Some credit providers did suggest, however, that new rules dealing with the permitted content of credit reporting information should be contained in a code of conduct, rather than in the new *Privacy (Credit Reporting Information) Regulations*.

56.9 In this context, the Australasian Retail Credit Association (ARCA) proposed that—while the regulations should restrict credit reporting information to that relevant to the primary purpose of the credit reporting system—permitted content should be governed by a code of conduct 'to ensure sufficient flexibility is maintained to meet the needs of a more rapidly changing credit environment'.[3] The Australian Finance Conference (AFC) commented that rather than be fixed in law, 'credit report content should be left to be negotiated by the stakeholders on the basis of known consequences'.[4]

56.10 In the ALRC's view, the permitted content of credit reporting information should continue to be prescribed by regulation. This approach is consistent with the overall approach to reform, under which the credit reporting provisions of the *Privacy Act* are repealed and regulations promulgated to impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information.[5]

56.11 The ALRC recommends that, as is presently the case under Part IIIA of the *Privacy Act*, the new *Privacy (Credit Reporting Information) Regulations* should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information. This should be based on the provisions of s 18E of the *Privacy Act*, subject to the changes recommended in this Report.

---

3 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.
4 Australian Finance Conference, *Submission PR 398*, 7 December 2007.
5 See Rec 54–1. For a detailed discussion of the regulatory model adopted by the ALRC, see Ch 4.

56.12 The specific permitted content of credit reporting information has, however, been subject to a range of comment and criticism. This is discussed below, with reference to different categories of content. The issue of more comprehensive reporting is discussed in Chapter 55.

Recommendation 56–1 The new *Privacy (Credit Reporting Information) Regulations* should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information. This list should be based on the provisions of s 18E of the *Privacy Act*, subject to the changes set out in Recommendations 55–1, 55–2, 56–2 to 56–4, 56–6, 56–8 and 56–9.

Identifying information

56.13 A credit information file may contain information that is 'reasonably necessary … to identify the individual'.[6] Under s 18E(3), the Privacy Commissioner has determined that credit information files may contain: an individual's full name, including any known aliases, sex, and date of birth; a maximum of three addresses consisting of a current or last known address and two immediately previous addresses; the name of the individual's current or last known employer; and the individual's driver's licence number.[7]

56.14 The identifying information included in credit information files is important as it affects the value of credit reporting information for non-credit related purposes, such as identity verification, and the accuracy of credit reporting because identifiers are used to match credit reporting records.[8] These issues are discussed further in Chapters 57 and 58.

Inquiry information

56.15 A credit information file may include information about an individual having applied to a credit provider for credit and the amount of credit sought in the application.[9] For the purposes of this Report, this information is referred to as 'inquiry information'. In addition, the *Credit Reporting Code of Conduct* states that 'a general indication of the nature of the credit being sought' also may be included.[10] Currently, however, whether the credit was granted cannot be recorded.

---

6 *Privacy Act 1988* (Cth) s 18E(1)(a).

7 Privacy Commissioner, *Determination under the Privacy Act 1988: 1991 No 2 (s 18E(3)): Concerning Identifying Particulars Permitted to be Included in a Credit Information File*, 11 September 1991.

8 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.

9 *Privacy Act 1988* (Cth) s 18E(1)(b)(i).

10 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [1.1].

56.16 Stakeholders expressed concern about the role of inquiry information in credit risk assessment.[11] Consumer credit caseworkers noted that some of their clients had been unfairly declined credit on the basis of multiple inquiry listings, including those attributable to 'shopping around' for credit cards or changing telecommunications service providers.[12] It was submitted that inquiry information relating to services (such as telecommunications) should only appear 'as an audit trail' and should not generally be used in credit risk assessment.[13]

56.17 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC noted that more comprehensive credit reporting would allow inquiry information to be matched with information about credit granted. Accordingly, inquiry information might no longer be as open to misinterpretation or relied on to the same extent in credit risk assessment. The ALRC asked for comment on: the role of inquiry information under the proposed comprehensive credit reporting scheme; and whether any other reform relating to the collection, use or disclosure of inquiry information was desirable.[14]

56.18 The Office of the Privacy Commissioner (OPC) stated that, if more comprehensive credit reporting were to be introduced, inquiry information would no longer be needed as part of credit risk assessment and, therefore, should not be given to credit providers. Credit providers and credit reporting agencies, however, should be required to log access to the individual's credit reporting information.[15]

56.19 In contrast, Optus submitted that it was essential to retain inquiry information in credit reports, even if more comprehensive credit reporting is introduced, because of the link between a high number of listed inquiries and credit default. It stated that

> inquiry information is not the sole indicator on which decisions are based, but it is certainly one of the criteria used. Multiple inquiries can simply be an indicator that a customer is shopping around for the best deal, but they can also be an indicator of declined credit applications by other providers. For this reason, Optus supports the maintenance of the existing rules in this regard, allowing inquiry information to appear on credit reporting files.[16]

---

11 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007; L Lucas, *Submission PR 95*, 15 January 2007.

12 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 85–89.

13 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 10.

14 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [52.25].

15 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

16 Optus, *Submission PR 532*, 21 December 2007.

ALRC's view

56.20 There is no compelling reason to prevent inquiry information from being reported if more comprehensive credit reporting is implemented. Credit reporting systems are currently structured to provide this information and inquiry information needs to be collected by credit reporting agencies, even if not reported to credit providers as a record of access (a basic data security safeguard).

56.21 It is widely accepted that individuals with more inquiries on their credit report are statistically more likely to default in the future than those with less.[17] A series of applications for personal loans within a short time, for example, often precedes bankruptcy.

56.22 The ALRC accepts that, due to this statistical relationship, inquiry information may disadvantage individuals who have multiple inquiries for other reasons than financial stress. Any such disadvantage, however, will be minimised under more comprehensive credit reporting because the presence of other data items will result in relatively less weight being given to inquiry information.

'Negative' information

56.23 The permitted content of credit information files and credit reports includes a range of 'negative' information. Stakeholders raised a number of concerns about permitted content relating to: small overdue payments; dishonoured cheques; bankruptcy and similar information; and serious credit infringements.

Small overdue payments

56.24 Section 18E(1)(b)(vi) permits the inclusion in credit information files of information about credit where the individual is at least 60 days overdue in making a payment and the credit provider has taken steps to recover the amount outstanding.

56.25 The credit reporting provisions do not provide for any minimum amount in respect of debts that may be listed, except in the case of presented and dishonoured cheques (discussed below). Veda Advantage, however, currently only lists debts over $100 and credit providers generally do not object to such a limit.

56.26 Some stakeholders expressed concerns about the listing of small debts, including by telecommunications companies. In particular, the consequences of listing small debts far outweigh the gravity of the conduct— especially as many small debts are said to be related to problems with billings systems, billing errors and change of address notification.[18]

---

17 See, eg, Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 86.

18 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

56.27 The extent to which small debts are predictive of future default is relevant to the desirability of imposing a minimum amount for the listing of overdue payments. Research conducted by Dun and Bradstreet, which focuses on telecommunications debts, claims to show that individuals who default on low value amounts (ie, amounts below $500) or non-bank credit are at higher risk of defaulting on larger amounts provided under more traditional credit arrangements.[19] Research by Dun and Bradstreet is also said to show that individuals 'defaulting on utilities and telecommunications debt are more than five times more likely to default on other credit products'.[20]

56.28 In DP 72, the ALRC proposed that credit reporting agencies should only be permitted to list overdue payments of more than a minimum amount.[21] The ALRC also asked whether the new *Privacy (Credit Reporting Information) Regulations* should prescribe this amount and, if not, how a minimum amount should be set and enforced.[22]

56.29 A wide cross-section of stakeholders supported the proposal to set a minimum amount.[23] Some considered that, rather than being set by the new regulations, the minimum amount should be included in a credit reporting code,[24] or in an industry agreement.[25] A range of figures, from the existing $100 to $1,000, was suggested as an appropriate minimum.[26]

---

19 Dun & Bradstreet Australasia, 'Low Value Defaults are a High Risk Equation' (2006) 5 *Consumer Credit Reporting* 2.

20 J Phillips, 'Non-bank Debt Defaulters Likely to Reoffend', *The Sheet*, 27 September 2007.

21 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–2.

22 Ibid, Question 52–1.

23 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; National Legal Aid, *Submission PR 521*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

24 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

25 Australian Credit Forum, *Submission PR 492*, 19 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

26 For example: $100: Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; $200: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; $500: National Legal Aid, *Submission PR 521*, 21 December

56.30 ARCA agreed that the reporting of overdue payments should be subject to a minimum, and that this limit should be incorporated in a credit reporting code, reviewed from time to time by a policy committee.[27] Similarly, Veda Advantage submitted:

> The Regulations should impose an obligation to collect and share data according to the regulations and the Code. But the Code rather than the Regulations should set the minimum amount for overdue payments. It should be enforced as part of the data standards of the industry. Breaches of the Code can be dealt with by the industry, but if persistent or serious, would be dealt with by the Privacy Commissioner under the Civil Penalty provisions.[28]

56.31 The AFC submitted a minimum amount should be

> applied through subscriber agreements between the credit provider and agency rather than subject to a Regulation … it is essential for credit providers to have a complete picture of the credit history of the individual including their propensity for paying debt that may be evidenced by the listing of relatively small overdue amounts. The agency is in the best position to track appropriate minimum levels and react to shift the level to reflect the current market as and when required.[29]

56.32 The Law Society of New South Wales agreed with the proposal only to list overdue payments over a certain amount, but also emphasised the importance of industry input into the process of determining the amount.

> Factors such as the volume of credit provided, the emergence of further forms of credit and the abilities of individuals to service credit are important for determining a suitable minimum amount for listing of overdue payments and the form in which the minimum amount should be expressed.[30]

56.33 Legal Aid Queensland considered that the minimum should be set at $500 and indexed against the Consumer Price Index. It noted that because 'consumers cannot access mainstream lending for any purposes if they have a default', the minimum of $100 proposed by industry 'does not properly balance the severe detriment caused by a small listing'.[31]

56.34 In contrast, the Australian Credit Forum noted that 'unpaid smaller debts can be a realistic guide of an individual's ability or intention to meet obligations and should be allowed to be taken into account in any credit risk assessment'.[32] The Tasmanian

---

2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007; $1,000: Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

27 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

28 Veda Advantage, *Submission PR 498*, 20 December 2007.

29 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

30 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

31 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

32 Australian Credit Forum, *Submission PR 492*, 19 December 2007.

Collection Service (a credit reporting agency) referred to a 'continued need' to collect information on small debts, particularly as a debt recovery mechanism.[33]

56.35 Telstra, Optus and AAPT stressed that any increase in the current minimum amount for listing overdue payments would have a disproportionate impact on the telecommunications industry, as many telecommunications debts are small.[34] Some stakeholders, including AAPT, were opposed to any mandatory minimum.[35] AAPT stated:

> Whilst such a proposal may be appropriate in some industries, it is not possible in the telecommunications sector. The telecommunications industry is a highly competitive industry and there is a well known and understood risk that consumers regularly run up small debts with multiple suppliers and switch between the different suppliers on a regular basis.[36]

ALRC's view

56.36 Different views were expressed by industry and consumer groups about the benefits and problems involved in reporting small debts. Consumer groups focused on the disproportionate consequences of reporting small overdue payments, while credit providers highlighted the significance of small debts in relation to credit risk assessment.

56.37 There is significant support, nevertheless, from both industry and consumer stakeholders for the imposition of some minimum amount for the reporting of overdue payments. While there were differing views on the mechanism for imposing a limit, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should provide for a prescribed minimum amount for overdue payment listings. This amount should be set following further consultation on the content of the new regulations. A valid alternative would be to leave the question to self-regulation by credit providers and credit reporting agencies, with consumer group input, through the credit reporting code.

56.38 In addition, some of the problems caused by the listing of small overdue payments can be addressed by other mechanisms, such as improved data quality and complaint-handling processes. The inclusion of repayment performance information in

---

33 Tasmanian Collection Service, *Submission PR 375*, 5 December 2007.

34 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

35 Australian Collectors Association, *Submission PR 505*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Tasmanian Collection Service, *Submission PR 375*, 5 December 2007.

36 AAPT Ltd, *Submission PR 338*, 7 November 2007.

credit reporting information, as recommended by the ALRC,[37] may also mean that smaller defaults play a less significant role in credit assessment.

Recommendation 56–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies are not permitted to list overdue payments of less than a prescribed amount.

Dishonoured cheques

56.39 Section 18E(1)(b)(vii) of the *Privacy Act* permits the listing on credit information files of information that is a record of a twice presented and dishonoured cheque for an amount of not less than $100. In DP 72, the ALRC proposed that the *Privacy (Credit Reporting Information) Regulations* not permit credit reporting information to include information about presented and dishonoured cheques.[38]

56.40 Industry stakeholders generally opposed this proposal.[39] ARCA submitted that the ability to report dishonoured cheques should be retained for the benefit of responsible lending, as 'it is highly predictive information in the case of repeated dishonours'.[40]

56.41 Similarly, the AFC stated that

> this subset of information relating to cheques is highly predictive information in the case of repeated dishonours. If the issue is the integrity of the database in relation to this information, we submit that the focus should be on improving the quality of the provision of this type of information. [41]

56.42 Other stakeholders, including the OPC and the Banking and Financial Services Ombudsman agreed that the listing of presented and dishonoured cheques should be prohibited.[42] Nigel Waters of the Cyberspace Law and Policy Centre stated that:

---

37 See Rec 55–2.

38 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–3.

39 Veda Advantage, *Submission PR 498*, 20 December 2007; Australian Credit Forum, *Submission PR 492*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. The Law Society of New South Wales submitted that dishonoured cheques should be able to be reported in repeat cases: Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

40 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. GE Money agreed with the ARCA position: GE Money Australia, *Submission PR 537*, 21 December 2007.

41 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

42 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

> If it were determined, and widely known, that dishonoured cheques are 'credit', there is the potential for almost any individual or organisation to be a 'credit provider' and gain access to [credit information files]. This would allow a major expansion of consumer credit reporting well beyond the relatively constrained limits, and beyond the policy objectives of the legislation.[43]

ALRC's view

56.43 The credit reporting system is based on the reporting of individuals' histories in relation to 'credit'. That term is defined in the *Privacy Act* to mean a 'loan'.[44] A loan includes an arrangement under which full payment for goods and services is not made.[45] It is doubtful whether payment for goods or services by cheque would constitute 'credit'.

56.44 This does not, of course, dispose of the issue because other content permitted expressly under Part IIIA includes items that are not 'credit'—such as court judgments and bankruptcy orders.[46] These items, however, are generally publicly available information.

56.45 The listing of presented and dishonoured cheques is anomalous and should no longer be permitted. In practice, dishonoured cheques are rarely listed with credit reporting agencies[47] and are increasingly irrelevant as a payment mechanism,[48] so this should not constitute any significant change to the existing credit reporting system.

Recommendation 56–3 The new *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques.

Personal insolvency information

56.46 Section 18E(1)(b)(ix) of the *Privacy Act* permits information about 'bankruptcy orders made against the individual' to be included in credit information files. The Act does not define the term 'bankruptcy order' and the term is not used in bankruptcy legislation.

---

43 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007

44 See *Privacy Act 1988* (Cth) s 6(1), definition of 'credit'.

45 See Ibid s 6(1), definition of 'loan'.

46 Ibid s 18E(1)(viii)–(ix).

47 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

48 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.

56.47 Under the *Bankruptcy Act 1966* (Cth), a person may become bankrupt upon the making of a sequestration order by the Federal Court following the presentation of a creditors' petition.[49] However, bankruptcy does not always require the making of an order against an individual. For example, bankruptcy can occur following the acceptance of a debtors' petition by the Official Receiver.[50] The *Bankruptcy Act* also provides, as alternatives to bankruptcy, debt agreements under Part IX and personal insolvency agreements under Part X.

56.48 A number of stakeholders suggested that the term 'bankruptcy order' should be clarified.[51] The AFC, for example, referred to an increase in the incidence of Part IX debt agreements.[52] While it recognised that 'a debt agreement has different connotations to a bankruptcy order insofar as it reflects a different attitude of a customer towards the repayment of their debt', the AFC recommended that

> either the definition of bankruptcy order be amended or a new definition of Part IX & Part X information be included in the Act to clarify that debt agreement and Part X personal insolvency agreement information can be included on a customer's credit information file.[53]

56.49 The Insolvency and Trustee Service Australia (ITSA) stated that, in practice, credit reporting agencies and credit providers interpret this term as including voluntary arrangements under Part IX and Part X, as well as bankruptcy proper.[54] The arguments against reporting debt agreements include that debtors should be encouraged to enter into debt agreements and an incentive for doing so is that some of the public 'stigma' of personal insolvency will be ameliorated. On the other hand:

> A debt agreement can be used only by a debtor who is insolvent and is a formal insolvency administration under the bankruptcy legislation which allows the debtor's debts to be compromised. This means creditors are paid less than the full amount of their debts and this information should be available to all creditors in the future.[55]

56.50 ITSA concluded that the 'policy reasons which support the public notification of bankruptcy … apply equally to debt agreements' and that if one aim of credit reporting is to ensure that 'fewer persons face financial difficulties' then reporting of debt agreements should be supported. ITSA also expressed concerns about the accuracy and

---

49 See *Bankruptcy Act 1966* (Cth) pt IV, s 43(2).

50 See Ibid pt IV, s 55(4A).

51 Australian Finance Conference, *Submission PR 294*, 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Min-it Software, *Submission PR 236*, 13 March 2007; Insolvency and Trustee Service Australia, *Submission PR 235*, 12 March 2007.

52 Approximately 6,500 new debt agreements were made between 1 July 2006 and 30 June 2007, compared with just under 5,000 debt agreements in the 2005–06 financial year: P Ruddock (Attorney-General), 'Amendments to Support Debt Agreements Commence' (Press Release, 9 July 2007).

53 Australian Finance Conference, *Submission PR 294*, 18 May 2007.

54 Insolvency and Trustee Service Australia, *Submission PR 235*, 12 March 2007.

55 Ibid.

completeness of personal insolvency information recorded on credit reports, if credit reporting agencies do not fully report individuals' insolvency status.[56]

ALRC's view

56.51 The term 'bankruptcy orders' does not appear to reflect all the types of personal insolvency administration available under the *Bankruptcy Act*. In addition to bankruptcies, including voluntary debtor's petitions and deceased estates administered in bankruptcy, the *Bankruptcy Act* provides for voluntary arrangements with creditors under Part IX and Part X and post-bankruptcy administration.[57]

56.52 All these forms of administration are currently recorded on the National Personal Insolvency Index (NPII).[58] The NPII is the source of bankruptcy information collected by credit reporting agencies.[59] Credit reporting information should be permitted to include all categories of information available on the NPII. Such information is important in credit risk assessment and, in practice, credit providers rely on obtaining this from credit reporting agencies rather than directly from the NPII.[60]

56.53 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the NPII; and that credit reporting agencies, in accordance with obligations to ensure the accuracy and completeness of credit reporting information, should ensure that credit reports adequately differentiate the forms of administration identified on the NPII.[61] These proposals met with general acceptance from stakeholders[62] and are confirmed in the recommendations set out below.

---

56 Ibid.

57 See, *Bankruptcy Act 1966* (Cth) pt VI, div 6.

58 The NPII is established and maintained in accordance with the *Bankruptcy Regulations 1996* (Cth) pt 13.

59 The content of searches on the NPII will ordinarily show: type of administration or proceeding; date of administration or proceeding; identification number; full name and alias of debtor; address of debtor; date of birth of debtor; occupation and business name of debtor; name of trustee or controlling trustee; particulars of any prior or subsequent listing; the end date of the administration: Insolvency and Trustee Service Australia, *National Personal Insolvency Index* (2007) <www.itsa.gov.au> at 5 May 2008.

60 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

61 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 52–4, 52–5.

62 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

Recommendation 56–4 The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index administered under the *Bankruptcy Regulations 1966* (Cth).

Recommendation 56–5 Credit reporting agencies should ensure that credit reports adequately differentiate the forms of administration identified on the National Personal Insolvency Index (NPII); and accurately reflect the relevant information recorded on the NPII, as updated from time to time.

Serious credit infringements

56.54 Section 18E(1)(b)(x) permits the inclusion in credit information files of the 'opinion of a credit provider that the individual has … committed a serious credit infringement'. A serious credit infringement is defined as an act done by a person:

> (a) that involves fraudulently obtaining credit, or attempting fraudulently to obtain credit; or
>
> (b) that involves fraudulently evading the person's obligations in relation to credit, or attempting fraudulently to evade those obligations; or
>
> (c) that a reasonable person would consider indicates an intention, on the part of the first-mentioned person, no longer to comply with the first-mentioned person's obligations in relation to credit.[63]

56.55 A serious credit infringement listing has more serious consequences for the individual concerned than other default listings—not least because such a listing may remain on the record for seven years, as compared to five years for most other negative information.

56.56 At the same time, listing a serious credit infringement under s 18E(1)(b)(x)(c) is not subject to the pre-conditions that apply to listing an overdue payment. That is, for an overdue payment to be listed on a credit information file, an individual must be 60 days overdue in making a payment, and the credit provider must have taken recovery action.[64]

56.57 The *Credit Reporting Code of Conduct* provides some guidance on what constitutes a serious credit infringement.[65] The Code states, for example, that what could reasonably be considered an intention on the part of an individual no longer to comply with credit obligations may include:

> - the individual has stopped making payments under a credit agreement/contract or breached it in some other serious way, and the credit

63 *Privacy Act 1988* (Cth) s 6(1).
64 Ibid s 18E(1)(vi).
65 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [62]–[65].

> provider has made reasonable efforts to contact the individual either in person or in writing, but has been unsuccessful in establishing contact, or
>
> - the credit provider has made contact with the individual and the individual has unlawfully refused to meet his or her credit obligations by resuming payments, or
> - the individual does not comply with the terms of a debt judgment.[66]

56.58 There are concerns about the interpretation of the current definition.[67] In DP 72, the ALRC asked whether the *Privacy (Credit Reporting Information) Regulations* should allow for the listing of a 'serious credit infringement' or similar event and, if so, how this concept should be defined.[68] Industry and consumer stakeholders supported retaining some concept of a 'serious credit infringement'.[69] Differing views remained on how the definition should be drafted.

56.59 The practice of listing a serious credit infringement against individuals who cannot be found by a credit provider ('clearouts'), without further inquiry, was criticised by consumer and privacy advocates.[70] Legal Aid Queensland observed:

> Often when people move they disconnect utility services and then realise often months later that they have not received a final bill or because of time lags in billing believe they have finalised the account or because they have reconnected with the

---

66 Ibid, [65].

67 Australian Finance Conference, *Submission PR 294*, 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 29; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

68 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 52–2.

69 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Credit Forum, *Submission PR 492*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007 National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. Some stakeholders suggested no change to the current definition was required: Australian Collectors Association, *Submission PR 505*, 20 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

70 See, eg, Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

> same service provider cannot understand why any outstanding accounts relating to the old address are not sent to the new address. In those circumstances a serious credit infringement is listed against the consumer. The other significant issue is that credit providers list a serious credit infringement against consumers who challenge the validity of the debt in its entirety or challenge that there is a default in payment.[71]

56.60 Consumer groups and others submitted that a narrow definition of 'serious credit infringement' is desirable and, in particular, that the concept should be limited to conduct that is fraudulent.[72] The Cyberspace Law and Policy Centre, for example, stated that

> there should be no direct replication of the item (c) from s 18E(1)(b)(x)—'reasonable suspicion' is too subjective. We further suggest that authority to list serious credit infringements should be contingent on membership of an approved EDR scheme … [73]

56.61 Other stakeholders supported placing some obligation on credit providers to make reasonable efforts to contact the individual concerned.[74] ARCA submitted, for example, that a 'serious credit infringement' should mean

> an act done by a person that a reasonable person would consider indicates an intention, on the part of the first-mentioned person, no longer to comply with the first person's obligations in relation to credit *and the provider has made an effort to contact the consumer*.[75]

56.62 The Australian Credit Forum stated that such listings are not made frequently because of concerns about 'misinterpretation or uncertainty'.[76] It submitted:

> Greater precision in the definition together with limitation of the liability of the listing party where it operated in good faith, or its actions to list were reasonable in the circumstances, may assist overcome this shortcoming.[77]

56.63 The OPC submitted that the definition of serious credit infringement should include individuals who are deemed to be acting with intent not to comply with their credit obligations, including those individuals who are 'clearouts'. The OPC submitted

---

71 Legal Aid Queensland, *Submission PR 489,* 19 December 2007.

72 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; National Legal Aid, *Submission PR 521,* 21 December 2007; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344,* 19 November 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

73 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007. Also Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

74 Banking and Financial Services Ombudsman, *Submission PR 471,* 14 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 29–30.

75 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007 (emphasis added). The ARCA position was supported explicitly by other stakeholders: eg, GE Money Australia, *Submission PR 537,* 21 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007.

76 Australian Credit Forum, *Submission PR 492,* 19 December 2007.

77 Ibid.

that it should issue guidance setting out the criteria that would need to be satisfied before a serious credit infringement may be listed, including:

> (a) How to define 'serious' (for example, has an overdue payment already been listed?);
>
> (b) Whether there needs to be a minimum timeframe in terms of days in default or a 'monetary threshold' before a serious credit infringement could be listed;
>
> (c) The positive obligations on credit providers and individuals towards proving/disproving that a serious credit infringement has occurred;
>
> (d) Whether there should be a restriction on listing a serious credit infringement where there is a dispute between the parties that is in the process of being resolved;
>
> (e) A requirement for a notice to be issued to the individual's last known address advising them that a serious credit infringement is to be listed against them.[78]

ALRC's view

56.64 The ALRC is not convinced that the concept of a serious credit infringement should be limited to conduct that is fraudulent, as suggested by some stakeholders. Credit providers have a legitimate interest in sharing information about the conduct of individuals that falls short of fraud—for example, where an individual deliberately avoids contact with a credit provider in order to evade his or her financial responsibilities.

56.65 Valid concerns remain, however, about the breadth of the current definition of a serious credit infringement. Currently, the definition is open to differing interpretations and has led to different practices governed by the internal policies of credit providers. The provision should at least require that, where conduct is not fraudulent, a credit provider must have taken reasonable steps to contact the individual before reporting a serious credit infringement.

56.66 It is not clear that the provision can be improved further by more detailed drafting. The solution to problems concerning the interpretation of the definition of 'serious credit infringement' lies in the provision of guidance for credit providers by the OPC or industry groups, or both. Some concerns about the serious credit infringement provision may be addressed, at least in part, by other changes to the regulation of credit reporting recommended in Chapters 58 and 59. A number of recommendations are intended, for example, to promote consistency and accuracy in reporting and improve complaint-handling and dispute resolution processes.

---

78 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

Recommendation 56–6 The new *Privacy (Credit Reporting Information) Regulations* should allow for the listing of a 'serious credit infringement' based on the definition currently set out in s 18E(1)(b)(x) of the *Privacy Act*, amended so that the credit provider is required to have taken reasonable steps to contact the individual before reporting a serious credit infringement under s 18E(1)(b)(x)(c).

Recommendation 56–7 The Office of the Privacy Commissioner should develop and publish guidance on the criteria that need to be satisfied before a serious credit infringement may be listed, including:

(a) how to interpret 'serious' (for example, in terms of the individual's conduct, and the period and amount of overdue payments);

(b) how to establish whether reasonable steps to contact the individual have been taken;

(c) whether a serious credit infringement should be listed where there is a dispute between the parties that is subject to dispute resolution; and

(d) the obligations on credit providers and individuals in proving or disproving that a serious credit infringement has occurred.

Publicly available information

56.67 The credit reporting provisions regulate some categories of publicly available information, but not others. The definition of a 'credit reporting business' excludes businesses or undertakings that maintain records 'in which the only personal information relating to individuals is publicly available information'.[79] On the other hand, the permitted content of a credit information file does not include 'publicly available information'—although some permitted items may be publicly available, such as bankruptcy and court judgment information.

56.68 The appropriateness of regulating some categories of publicly available information under Part IIIA, but not others, has been questioned. For example, if a credit reporting agency holds publicly available information about court judgments in separate records—rather than in credit information files—the information can be retained indefinitely as there are no specified time limits for retention under general

79 *Privacy Act 1988* (Cth) s 6(1). Part IIIA provides that credit reporting agencies and credit providers may disclose information contained in a record 'in which the only personal information relating to individuals is publicly available information': see *Privacy Act 1988* (Cth) ss 18K(1)(k), 18N(9) definition of 'report'.

privacy principles. If governed by Part IIIA, the information would have to be deleted five years after the judgment was made.[80]

56.69 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information.[81] This proposal received broad, but qualified, support from stakeholders.[82] It may, however, have been understood in different ways by stakeholders, given that the permitted content of credit information files already includes some categories of publicly available information.

56.70 Some industry stakeholders considered that, while publicly available information should be included in credit reporting information, it should not necessarily be regulated in the same way as credit reporting information, or subject to the new *Privacy (Credit Reporting Information) Regulations.* ARCA and others, for example, expressed concern that publicly available information should not be regulated as credit reporting information by virtue simply of being held by a credit reporting agency.[83]

56.71 The AFC opposed the proposal and submitted that

> credit reporting information should not be defined to include publicly available information (eg bankruptcy information, default judgment information). We do not see the outcome of this being that a credit reporting agency cannot collect and distribute this information to credit providers, but that its handling by these entities would be subject to the broader UPPs. Given the statutory framework for the creation and regulation of the entity collecting and distributing the information (eg generally government agencies like ITSA, ASIC) and the statutory privacy protections that apply to this handling, we see no reason for applying a higher standard of collection than the UPPs. The credit reporting agency effectively [acts] as a conduit between the government agency and the requesting entity.[84]

56.72 Other stakeholders also addressed issues arising from the possible inclusion of publicly available information in credit reporting information. The Cyberspace Law and Policy Centre submitted that publicly available information 'whether held in credit

---

80 *Privacy Act 1988* (Cth) s 18F(2)(e).

81 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–6.

82 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

83 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; GE Money Australia, *Submission PR 537*, 21 December 2007.

84 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

information files or separately, should be regulated by the credit reporting Regulations if and when it is brought together with other information for the purposes of a credit report'.[85]

56.73 The OPC agreed that the new regulations should permit credit reporting information to include publicly available information, but noted that not all publicly available information is relevant for credit reporting purposes. The OPC submitted that 'the categories of publicly available information that will be permitted content in the credit reporting system should be set out as an exhaustive list' in the regulations.[86]

56.74 Legal Aid Queensland submitted that publicly available information provided by a credit reporting agency to a credit provider for the purpose of assessing an individual's credit worthiness should fall within the definition of 'credit reporting information'. This would ensure that individuals can challenge the relevance of the information, and that information is deleted after the expiry of the maximum permissible periods set out in credit reporting regulation.[87]

ALRC's view

56.75 Where publicly available information is used in consumer credit reporting, it is appropriate that privacy interests in respect of this information are fully protected by, for example, the application of the special rights of access and correction that apply to credit reporting information, and complaint-handling mechanisms.

56.76 The existing categories of publicly available information permitted under s 18E—bankruptcy (personal insolvency) and court judgment information—should be included in the list of permitted content of credit reporting information under the new *Privacy (Credit Reporting Information) Regulations*.

56.77 No case has been made for the inclusion of other categories of publicly available information in credit reporting information. The new regulations, therefore, should not permit credit reporting information to include all publicly available information, as proposed in DP 72.[88]

56.78 As discussed in Chapter 54, the new *Privacy (Credit Reporting Information) Regulations* should ensure that publicly available information maintained by a credit reporting agency is covered by credit reporting regulation only where the information is maintained 'in the course of carrying on a credit reporting business'. As is presently the case, a credit reporting agency should be able to conduct other business undertakings using publicly available or other personal information that it holds, subject to compliance with the UPPs and other obligations under the *Privacy Act*.

---

85 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

86 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

87 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

88 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–6.

Prohibited content of credit reporting information

56.79 Section 18E(2) provides that certain types of personal information must never be included in an individual's credit information file. This list is similar to, but differs in some respects from, the general definition of 'sensitive information' in s 6(1).

56.80 First, the definition of prohibited content in s 18E(2) includes personal information recording an individual's 'lifestyle, character or reputation', which is not specifically an element of the definition of sensitive information.[89] Secondly, the definition of sensitive information includes 'health information', which is not referred to in s 18E(2). In addition, the ALRC recommends that the definition of 'sensitive information' in the *Privacy Act* be amended to include biometric information collected for the purpose of automated biometric verification or identification; and biometric template information.[90]

56.81 The concepts of prohibited content under s 18E(2) and sensitive information under s 6(1) serve quite distinct purposes. The former, in effect, acts to prohibit collection (with or without the consent of the individual); the latter to restrict collection without consent, and limit use or disclosure for secondary purposes.[91]

56.82 In response to the Issues Paper, *Review of Privacy* (IP 31), the OPC suggested that the ALRC consider whether the prohibited content set out in s 18E(2) should be the same as the 'sensitive information' in s 6(1) of the *Privacy Act*.[92] In DP 72, the ALRC proposed that the *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as that term is defined in s 6(1) of the *Privacy Act*.[93] Stakeholders who addressed the issue were unanimous in their support for the proposal.[94]

---

89 *Privacy Act 1988* (Cth) s 18E(2)(f).

90 Rec 6–4.

91 In conjunction with NPPs 10 and 2.1.

92 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

93 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. The Cyberspace Law and Policy Centre and the Australian Privacy Foundation suggested that the ALRC recommend the Regulations prohibit the inclusion in credit reporting information of 'sensitive information' and information about an individual's 'lifestyle, character or reputation'.

94 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–7.

56.83 If an equivalent of s 18E(2) is to be included in the new regulations, it would make sense to align the provision with the definition of 'sensitive information' for the sake of consistency and to simplify the drafting of the regulations.

56.84 The need expressly to prohibit the collection of a defined category of sensitive information in credit reporting remains questionable given that this information would not be permitted content under the new *Privacy (Credit Reporting Information) Regulations*. There is some possibility, however, that the collection of sensitive information might otherwise be permissible under the new regulations. It is conceivable, for example, that some content permitted under the regulations may constitute health information—for example, a record of an overdue payment owed to a hospital or doctor. On the other hand, credit reporting information would not ordinarily be specific enough to constitute information 'about' the individual's health (as opposed to about the fact an individual owes money to a health service provider).

56.85 It is also possible that biometric template information might be used for identifying individuals in the context of credit application or reporting processes. As noted above, the ALRC recommends that the definition of sensitive information include biometric template information.[95] Expressly prohibiting the collection in credit reporting information of 'sensitive information' would mean that biometric template information could not be included as a permitted identifier by a determination of the Privacy Commissioner under existing s 18E(3)—as is theoretically the case now.

Recommendation 56–8 The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as defined in the *Privacy Act*.

Debts of children and young people

56.86 There are concerns about credit reporting information about individuals under the age of 18—especially in relation to the listing of debts by telecommunication companies in relation to mobile telephone contracts.[96]

56.87 A 'protective' approach is reflected in the common law, where contracts are not binding on a person under the age of 18 unless it is a contract for 'necessaries'. The common law applies in all Australian states and territories except New South Wales, where legislation has modified the common law position. Legislation in New South Wales focuses on the contract being for the 'benefit' of the child or young person,

95 Rec 6–4.

96 See Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.141]–[5.147].

where the child or young person is sufficiently mature to understand his or her participation in the contract.[97]

56.88 While many companies are mindful of how the law of contract applies to those under the age of 18—and many mobile telephone contracts are signed by adults on behalf of young people—young people, nevertheless, regularly purchase mobile telephones in their own name or sign contracts for future telecommunications services in their own name.[98] Other young people may enter contracts with banks or other financial institutions for loans or credit cards. While some seek loans or credit facilities due to the need to live independently, others may complete offers for credit cards inadvertently sent to them as part of a marketing campaign. Other young people may accumulate a debt by not paying a fine, such as a parking fine, or a fine issued for a public transport ticket violation.[99]

56.89 Where credit obligations are not discharged, telecommunications companies and other credit providers may list overdue payment information with a credit reporting agency. Such information can remain on the individual's credit information file for up to five years and prejudice a young person's future access to credit. This may be the case even where the legality of the contract is in question.

56.90 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals the credit provider or credit reporting agency knows to be under the age of 18 years.[100]

---

97 *Minors (Property and Contracts) Act 1970* (NSW). Some limited exceptions to the common law apply in the other states and territories: see L Blackman, *Representing Children and Young People: A Lawyers Practice Guide* (2002), 240.

98 A 1999 Australian study indicated that 48% of young people under the age of 18 with a mobile telephone signed the contract in their own name: A Funston and K MacNeill, *Mobile Matters: Young People and Mobile Phones* (1999) Communications Law Centre, 3. Note, however, that in 2005 most telecommunications companies commenced using a new form of contract requiring disclosure of age and not allowing persons under the age of 18 to sign the contract in their own name: Children and Young People Issues Roundtable, *Consultation PC 121*, Sydney, 7 March 2007.

99 New South Wales Commission for Children and Young People, *Consultation PC 34*, Sydney, 18 July 2006.

100 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–8.

56.91 Most stakeholders who addressed the issue supported the proposal.[101] Some stakeholders suggested that credit reporting agencies should also be required to delete information about individuals over the age of 18, on being notified that credit was granted or the information listed when those individuals were known (or should have been known by the credit provider) to be under the age of 18.[102]

56.92 Some stakeholders suggested that there should be some exceptions to the general prohibition on the collection of credit reporting information about individuals under the age of 18. The AFC stated, for example, that 'some qualification may be required for special cases where establishing a credit report for the child may be advantageous to them (eg for teenagers living independently)'.[103]

56.93 The OPC submitted that the new regulations should permit the collection of information about individuals under the age of 18, but make 'adverse credit listing timeframes shorter, for example 2 years for payment defaults and 4 years for serious credit infringements'. The OPC also suggested that, as an alternative, credit providers and credit reporting agencies could be required to delete credit reporting information about an individual when the individual reaches the age of 18 years.[104]

56.94 The collection of credit reporting information about individuals under the age of 18 should be prohibited. Any regulation to this effect, however, would have to recognise that credit providers and credit reporting agencies may not always know the age of individuals in relation to whom information is collected. The ALRC recommends, therefore, that the new regulations should prohibit the collection of credit reporting information about individuals who the credit provider or credit reporting agency knows, or *reasonably should know*, to be under the age of 18 years.

---

101 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. Optus opposed the proposal on the basis that its 'existing IT systems would be unable to exclude such records based on date of birth': Optus, *Submission PR 532*, 21 December 2007.

102 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007.

103 Australian Finance Conference, *Submission PR 398*, 7 December 2007. Dun and Bradstreet also referred to the position of consumers under the age of 18 who need to apply for credit in relation to utilities: Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007.

104 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

56.95 While it is possible that such a reform might have some undesirable effects, for example in prejudicing the ability of some younger people living independently, or those with parents with bad credit records, to obtain credit or services they need, this will be relatively rare. The 11 million files held by Veda Advantage include only 2,137 files on people under the age of 18.[105]

Recommendation 56–9 The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals who the credit provider or credit reporting agency knows, or reasonably should know, to be under the age of 18.

Notification of collection

56.96 The 'Notification' principle in the model UPPs provides that, at or before the time an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify or ensure that the individual is aware of the: fact and circumstances of collection where the individual may not be aware that his or her personal information has been collected; identity and contact details of the agency or organisation; rights of access to, and correction of, personal information provided by these principles; purposes for which the information is collected; main consequences of not providing the information; actual or types of organisations, agencies, entities or persons to whom the agency or organisation usually discloses personal information; fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and fact, where applicable, that the collection is required or authorised by or under law.

56.97 Part IIIA provides indirectly for notification. Under s 18E(8)(c), a credit provider must not give to a credit reporting agency personal information relating to an individual if 'the credit provider did not, at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a credit reporting agency'. It has been suggested that the words 'at the time of, or before, acquiring the information' may permit the credit provider a choice about when to provide notice to the individual that information may be disclosed. Given that a significant period may elapse between the relevant events, more prescriptive notice provisions may be appropriate.

105 Veda Advantage, *Submission PR 498*, 20 December 2007.

56.98 The interpretation of s 18E(8)(c) has been the subject of a representative complaint to the OPC, lodged in April 2006 by the Consumer Credit Legal Centre (NSW) and the Consumer Credit Legal Service Inc (Vic) against Baycorp Advantage Business Information Services Ltd and Alliance Factoring Pty Ltd.[106] The complaint relates to the listing of about 600,000 individuals for default or serious credit infringement, lodged by Alliance in relation to Telstra debts.

56.99 The complaint claims a failure to inform individuals that personal information might be disclosed to a credit reporting agency. The complainants submitted that the correct interpretation of s 18E(8)(c) is that an individual should be notified at the time of, or before, the handing over of personal information, and the relevant time is the time of the application for a loan, account or other relevant facility. The opposing argument is that a credit provider may comply with s 18E(8)(c) by notifying an individual that it intends shortly to list a default—and does not need to have notified the individual about this possibility at the time of the initial credit application.

56.100 The Consumer Action Law Centre contested the validity of the latter interpretation, which it considered 'has been developed to meet the interests of debt purchase firms and [credit reporting agencies] to maximise the listing of utility defaults'.[107] The Centre submitted that

> more prescriptive notice provisions may be appropriate, as they would in effect simply clarify the operation of the existing provision, namely that notice should be given at relevant times, for example at initial application stage, if a default is to be listed, if a debt is assigned and so on.[108]

56.101 The OPC noted that the notice provision in s 18E(8)(c) is important as it 'promotes transparency between the individuals, credit providers and to some extent credit reporting agencies'. The notice provision was said to generate a number of complaints, particularly in relation to assigned loans where, for example, notice may have been given a long time before a listing is made, or an assignee assumes notice has been provided by the original credit provider and does not provide notice at the time of listing.[109] The OPC recommended that s 18E(8)(c) be redrafted to 'align it more closely with the requirements under NPP 1.3, and to require that notice is given prior to any listing being made or a debt being assigned'.[110]

---

106 The Cyberspace Law and Policy Centre advised that the Privacy Commissioner has 'now formed a final view with which the complainant NGOs disagree, but has declined to make a formal Determination that could be challenged': Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

107 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

108 Ibid.

109 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

110 Ibid.

56.102 Submissions from a range of bodies favoured the imposition of more prescriptive notice requirements.[111] It was suggested that credit providers or credit reporting agencies should be required specifically to notify individuals about default listings and complaint-handling processes.[112] More prescriptive notice requirements were opposed by others.[113]

Discussion Paper proposal

56.103 In DP 72, the ALRC proposed that the *Privacy (Credit Reporting Information) Regulations* should provide that, at or before the time credit reporting information is collected about an individual, credit providers must take reasonable steps to ensure that the individual is aware of the:

- fact and circumstances of collection (for example, how and where the information was collected);
- credit provider's and credit reporting agency's identity and contact details;
- fact that the individual is able to gain access to the information;
- main consequences of not providing the information;
- types of people, organisations, agencies or other entities to whom the credit provider and credit reporting agency usually discloses credit reporting information; and
- avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her credit reporting information.[114]

56.104 The ALRC also proposed that the regulations should prescribe the specific circumstances in which a credit provider must inform an individual that personal information might be disclosed to a credit reporting agency, for example, in circumstances where the individual defaults in making payments.[115] It asked:

---

111 Queensland Law Society, *Submission PR 286*, 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007; Westpac, *Submission PR 256*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007.

112 Issues concerning the notification given when an individual's application for credit is refused on the basis of a credit report under s 18M of the *Privacy Act* are discussed in Ch 59.

113 For example, EnergyAustralia, *Submission PR 229*, 9 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007.

114 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–9.

115 Ibid, Proposal 52–10.

- In what specific circumstances should a credit provider be obliged to inform an individual that personal information might be disclosed to a credit reporting agency; and what information should notices contain? Who should give notice when a debt is assigned—the original credit provider, the assignee or both?[116]

- Should the regulations prescribe specific circumstances in which a credit reporting agency must inform an individual that it has collected personal information?[117]

Submissions and consultations

56.105 Most stakeholders accepted there is some need for specific rules regarding notification in credit reporting contexts.[118] Galexia noted, for example, that notification is a 'key privacy right once consent is removed as a privacy protection, and requirements for timely and effective notice need to be in the regulations in order to balance the removal of consent'.[119] The Cyberspace Law and Policy Centre submitted that the *Privacy (Credit Reporting Information) Regulations* should 'prescribe both the content and timing of notices by all relevant parties'.[120]

56.106 The OPC agreed that the regulations should provide that, at or before the time credit reporting information about an individual is collected, credit providers must take reasonable steps to ensure that the individual is aware of the matters set out in the ALRC's proposal. The OPC also submitted that a notice regarding the handling of an individual's credit reporting information could set out: the possible uses and disclosures that could occur during the credit relationship; a brief explanation of the operation of the credit reporting system; and that notice should be provided to the individual separate to other information about credit terms and conditions.[121]

56.107 Some stakeholders did not consider that notification of collection should be dealt with primarily in regulations. ARCA, for example, stated that it agreed with the 'basic principles of notification regarding collection and use' but submitted that the 'details regarding practical implementation' should be left to the code of conduct.[122]

---

116 Ibid, Question 52–3.

117 Ibid, Question 52–4.

118 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007; Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Australian Credit Forum, *Submission PR 492,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344,* 19 November 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007;

119 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.

120 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

121 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.

122 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007. See also National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007.

56.108 Other stakeholders submitted that there should not be any specific rules relating to notification of the collection of credit reporting information.[123] It was argued that the provisions of the general privacy principles, including the 'Notification' principle in the model UPPs, would provide adequate regulation.[124] Optus stated, for example, that regulating notification obligations would be

> contrary to the approach taken by the Government's taskforce in reducing the regulatory burden on business, which advocated for more high level regulations (not prescriptive rules which impact on providers' business processes) … By imposing a prescriptive list of scenarios when credit providers must give specified information to customers, regardless of that customer's individual circumstances, this will simply add to the information overload already experienced by consumers.[125]

56.109 Telstra considered that 'requirements relating to the notification of collection should be covered by the new UPPs' and that credit reporting regulations should simply replicate the current obligations in s 18(8)(c) of the *Privacy Act*.[126]

56.110 Some stakeholders supported further prescription of the circumstances in which a credit provider should be required to inform an individual that personal information might be disclosed to a credit reporting agency.[127] Other stakeholders opposed further prescription.[128] The Mortgage and Finance Association of Australia stated:

> It will be counter-productive to inform consumers of too much information. A general statement that personal and credit information may be provided to a credit reporting agency is sufficient to alert consumers to that matter.[129]

56.111 The AFC stated that, in considering the notification obligations to be incorporated in credit reporting regulations, other consumer credit compliance requirements, including under the *Consumer Credit Code*,[130] need to be taken into

---

123 Optus, *Submission PR 532*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

124 Veda Advantage, *Submission PR 498*, 20 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

125 Optus, *Submission PR 532*, 21 December 2007. Optus noted that an industry code could provide guidance on the provision of notices.

126 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

127 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Credit Forum, *Submission PR 492*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

128 Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

129 Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

130 The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories.

account. The *Consumer Credit Code*, for example, 'recognises that the issue of a default notice to a debtor prior to the credit provider taking recovery action is not always necessary'.[131] It argued that 'an upfront notice warning the debtor that a default may be listed may be sufficient' and a requirement for notice, prior to default listing, might operate against the public policy of the *Consumer Credit Code*.[132]

56.112 The timing of notices was also an important concern. Legal Aid Queensland submitted that the timing of notification should be 'spelt out either in the regulations or in the binding code' and be a 'continuing obligation dependant on what information is disclosed to the credit reporting agency and where the information is collected in the Financial Transaction Life Cycle'.[133] Similarly, the Australian Privacy Foundation submitted that, while it generally supported the proposed content of the regulation, 'it is still too ambiguous as to timing—it doesn't address contentious interpretation by the OPC which has allowed notice to be given at the time of a default listing by an assignee, even though there has been no initial notice'.[134]

56.113 The Cyberspace Law and Policy Centre also suggested that the new regulations need to be 'more prescriptive about the timing of notices' because it is unsatisfactory for individuals to be told about the possibility of a default listing only when they default or when a debt is assigned:

> For the notice requirement to have its intended effect, it needs to apply at the time an individual is still in a position to walk away from the transaction ie. at the time of initial application for credit. It should however also apply at key subsequent events such as prior to default listing and on assignment.[135]

56.114 Similarly, the Financial Counsellors Association of Queensland stated that:

> As well as the regulations specifying when credit providers should inform consumers regarding a listing to a credit reporting agency, credit providers should be providing that information at time of application for credit by a consumer. It has been our experience that credit providers need to ensure consumers are aware of their rights and obligations at time of credit application.[136]

56.115 Other stakeholders expressed concern about more prescriptive provisions dealing with the timing of notices. Telstra stated, for example, that an obligation to notify 'at or before' the time credit reporting information is collected is

> often not practical (for example, in the context of telephone contact). In Telstra's view the existing wording in NPP 1 (allowing the provision of the information 'as soon as practicable after') has worked well and means that individuals receive relevant information close to the time of collection.[137]

---

131 *Consumer Credit Code* s 80(4).
132 Australian Finance Conference, *Submission PR 398*, 7 December 2007.
133 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.
134 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
135 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
136 Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.
137 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

56.116 The Australian Credit Forum agreed that the circumstances of notification should be prescribed but submitted that this need not be 'at the time of a default but should instead be allowed to be included at the time of initial granting of credit' to address 'the difficulties in skip and fraud situations'.[138]

56.117 A number of consumer and industry stakeholders agreed that, in addition to notice at the first point of collection of credit reporting information (generally, when a credit application is made), individuals should be notified when a default is listed and when debt is assigned.[139]

56.118 The complexities involved in further prescription of notification obligations were highlighted by the views on the issue of notification when debt is assigned. ARCA and others stated that it should be the obligation of the assignee, at the time of the sale, to notify the consumer that the debt has been assigned.[140] Others considered notice should be provided to the individual by the assignor[141] or either (or both) the assignor and assignee.[142] The AFC stated that, in practice, which party gives notice depends on 'matters of contract, statute and general legal principles':

> For example, the form of the assignment, (ie equitable assignment vs. legal assignment) may impact on whether notice is given to the debtor at all. Where notice is to be given, the contract of assignment may cover whether the obligation to notify rests with the assignor (ie financier) or the assignee (ie debt collector). Therefore, any decision to impose notification obligations on either party, should take this into account. Further, the potential for a conflict of laws or the imposition of a dual notification obligation (eg at state level under the property laws and at the Commonwealth level under privacy laws) should be avoided because of the lack of identified customer protection benefit and attendant compliance costs that may result.[143]

56.119 There was little support for imposing notification obligations on credit reporting agencies. ARCA noted that the collection responsibility is with the credit provider and that

> the only circumstances where a [credit reporting agency] should provide notice to consumers that it has collected personal information are those circumstances where

---

138 Australian Credit Forum, *Submission PR 492*, 19 December 2007.

139 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

140 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. See also GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

141 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

142 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

143 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

> the consumer may have no other means of notice—that is, for information collected indirectly other than from credit providers. This category is almost exclusively public information. [Credit reporting agencies] should provide general rather than individual notice to consumers, for example in the form of tiered privacy notices.[144]

56.120 Credit reporting agencies already offer, for a fee, to notify individuals of additions or changes to their credit information files.[145] Veda Advantage has advised that it intends to develop the capacity to manage notification electronically and directly with consumers, where appropriate.[146]

ALRC's view

56.121 Provisions dealing with aspects of notification of collection should be incorporated in the new *Privacy (Credit Reporting Information) Regulations*. This approach received significant support. The proposal in DP 72 was, however, criticised by some stakeholders for duplicating the obligations contained in the existing NPP 1.3 and the 'Notification' principle in the model UPPs.[147] Duplication would be contrary to the ALRC's expressed view that the new regulations should be drafted to contain only those requirements that are different or more specific than provided for in the model UPPs.[148]

56.122 There are aspects of the notification obligations in respect to credit reporting that do not duplicate those in the 'Notification' principle. It is important, however, that the regulations require credit providers to inform individuals about information handling by credit reporting agencies. For example, while the 'Notification' principle obliges an organisation that collects personal information to ensure the individual concerned is aware of the 'actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information', what is required, in the context of credit reporting, is that credit providers also inform individuals about the types of organisations, agencies, entities or other persons to whom the credit reporting agency usually discloses personal information. Insofar as the 'Notification' principle applies to indirect collection, the principle does not achieve this end, because it places obligations on the credit reporting agency and not credit providers.

56.123 Another concern about duplication of obligations concerned the provisions of the telecommunications industry credit management code.[149] In the ALRC's view,

---

144 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. See also GE Money Australia, *Submission PR 537*, 21 December 2007.

145 See Ch 59.

146 Veda Advantage, *Submission PR 272*, 29 March 2007.

147 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

148 See Rec 54–2.

149 AAPT Ltd, *Submission PR 338*, 7 November 2007; Australian Communications Industry Forum, *Industry Code—Credit Management*, ACIF C541 (2006).

however, this does not constitute duplication; rather, the code states that it must be read in conjunction with Part IIIA and that telecommunications suppliers must comply with the provisions of Part IIIA.[150]

56.124 The 'Notification' principle refers to notification 'at or before the time (or, if that is not practicable, as soon as practicable after)' of collection. Section 18E(8)(c) contains the similar words 'at the time of, or before, acquiring the information'. Section 18E(8)(c) has been the subject of varying interpretation and lacks clarity in its application. For example, the drafting allows credit providers to argue that the obligation does not require:

- notification at the time of the initial credit application that a default might be listed in the future; or

- notification before or at the time a default listing is made, provided that notification (that a default might be listed in the future) was given at the time of the initial credit application.

56.125 The ALRC understands that giving notice immediately before listing a default has been adopted generally as good industry practice.[151] This practice should be mandated by the regulations.

Recommendation 56–10 The new *Privacy (Credit Reporting Information) Regulations* should provide, in addition to the other provisions of the 'Notification' principle, that at or before the time personal information to be disclosed to a credit reporting agency is collected about an individual, a credit provider must take such steps as are reasonable, if any, to ensure that the individual is aware of the:

(a) identity and contact details of the credit reporting agency;

(b) rights of access to, and correction of, credit reporting information provided by the regulations; and

(c) actual or types of organisations, agencies, entities or persons to whom the credit reporting agency usually discloses credit reporting information.

150 Australian Communications Industry Forum, *Industry Code—Credit Management*, ACIF C541 (2006), [1.1.4], App B.

151 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

Recommendation 56–11 The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit provider, before disclosing overdue payment information to a credit reporting agency, must have taken reasonable steps to ensure that the individual concerned is aware of the intention to report the information. Overdue payment information, for these purposes, means the information currently referred to in s 18E(b)(1)(vi) of the *Privacy Act*.

57. Use and Disclosure of Credit Reporting Information

Contents

Introduction

57.1 This chapter focuses on the existing provisions of Part IIIA of the *Privacy Act 1988* (Cth) dealing with the use and disclosure of credit reporting information. Recommendations are made on how these matters should be dealt with under the model Unified Privacy Principles (UPPs) and the new *Privacy (Credit Reporting Information) Regulations*.

Use and disclosure

57.2 Under the 'Use and Disclosure' principle in the model UPPs, an agency or organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

> (a) both of the following apply:
>
> (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
>
> (ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose; or
>
> (b) the individual has consented to the use or disclosure …

57.3 The relative simplicity of the general principle set out in clause (a), which permits use or disclosure for related secondary purposes within the reasonable expectation of the individual concerned, may be contrasted with the complexity of the use and disclosure provisions of Part IIIA.

57.4 Sections 18K, 18L, 18N, 18P and 18Q all deal with aspects of the use or disclosure of personal information (or both). These provisions place various limits on the use and disclosure of personal information based on the identity of the person or organisation to whom information is disclosed; the source and nature of the information; and the purpose for which the information is to be used. Briefly, the use and disclosure provisions of Part IIIA deal with the following:

- s 18K places limits on the disclosure by credit reporting agencies of personal information contained in credit information files;
- s 18L places limits on the use by credit providers of personal information contained in credit reports;
- s 18N places limits on the disclosure by credit providers of personal information in 'reports relating to credit worthiness';
- s 18P places limits on the use or disclosure by mortgage insurers or trade insurers of personal information contained in credit reports; and

- s 18Q places limits on the use of personal information obtained from credit providers by: a corporation that is related to the credit provider; a corporation that proposes to use the information in connection with an assignment or purchase of debt; or a person who manages loans made by the credit provider.[1]

Comparing Part IIIA and the NPPs

57.5 The Part IIIA provisions may operate to make use and disclosure of credit reporting information more or less restrictive than is the case under general privacy principles. The extent to which any particular category of use or disclosure permitted by Part IIIA also would be permitted by the National Privacy Principles (NPPs) or the model UPPs, however, is difficult to determine. The determination depends primarily on whether the specific circumstances in which use or disclosure is authorised by Part IIIA are related secondary purposes within the reasonable expectations of the individual.

57.6 How broadly an organisation can describe the primary purpose needs to be determined on a case-by-case basis and depends on the circumstances.[2] The Office of the Privacy Commissioner's (OPC) *Guidelines to the National Privacy Principles* state that when an individual provides, and an organisation collects, personal information, they almost always do so for a particular purpose. This is 'the primary purpose of collection even if the organisation has some additional purposes in mind'.[3]

57.7 Even on a broad conception of the term 'primary purpose', it is hard to argue that the disclosure of information by a credit provider to a credit reporting agency is for the primary purpose of collection. Disclosure does not directly serve purposes connected with the provision of finance by a credit provider to an individual. Rather, the information is disclosed so that it may be used in the future, including by other credit providers in assessing other loan applications. This conclusion has not been contested.

57.8 In the ALRC's view, for the same reasons, disclosure to a credit reporting agency is unlikely to be considered a related secondary purpose for the purposes of NPP 2.1(a) or the 'Use and Disclosure' principle in the model UPPs. This conclusion, however, has been contested. In a submission to the Inquiry, Nigel Waters of the Cyberspace Law and Policy Centre stated:

> It is suggested that it may be necessary for credit providers to obtain consent for disclosures involved in the credit reporting system because they would not fit within the alternative exception for secondary purposes … I submit that it is at least arguable that within the context of the well established operation of the credit market,

---

1 These provisions are summarised in more detail in Ch 53.
2 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 35.
3 Ibid, 35.

> disclosure to [credit reporting agencies] and other [credit providers] is both a related purpose and within reasonable expectations …[4]

57.9 These comments serve to highlight the fact that different conclusions can be reached even on the most basic questions about how NPP 2 applies to credit reporting information. In this context, the provisions of Part IIIA can be seen as providing some certainty for existing finance industry practices. The provisions remove the need to determine whether, for example, the disclosure by a credit provider of personal information to a credit reporting agency, a mortgage insurer, or the assignee of a debt to the credit provider are within the reasonable expectations of the individual concerned.

Use and disclosure of credit reporting information

57.10 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC observed that Part IIIA prescribes more than fifty different circumstances in which the use or disclosure of personal information is authorised.[5] As the categories of permitted use and disclosure are exhaustive, all other uses or disclosures of personal information are prohibited. Additional complexity arises because, in some instances, the provisions also limit the kinds of personal information that may be disclosed.[6]

57.11 Despite the extensive nature of these provisions, there may also be some gaps in their coverage. Notably, while the permitted content of credit information files held by credit reporting agencies and the disclosure of personal information contained in those files are regulated in detail by ss 18E and 18L respectively, Part IIIA does not limit expressly the use of credit information files by credit reporting agencies.

Discussion Paper proposal

57.12 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information, based on those uses and disclosures currently permitted under ss 18K, 18L and 18N of the *Privacy Act*.[7] It was proposed that the regulations provide that, in addition, a credit reporting agency or credit provider may use or disclose credit reporting information for related secondary purposes, as permitted by the 'Use and Disclosure' principle.[8]

---

4 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007.

5 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [53.5].

6 For example, s 18N(1)(be) permits the disclosure of personal information to a person or body supplying goods or services to an individual who intends to pay by credit card or electronic funds transfer. The information that may be disclosed is limited to information reasonably necessary to identify the individual, and to determine whether the individual has access to funds sufficient to meet the payment concerned.

7 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 53–1.

8 Ibid, Proposal 53–2.

Submissions and consultations

57.13 The Cyberspace Law and Policy Centre noted that divergent views on how privacy principles should apply to credit reporting information demonstrate the need for 'a more prescriptive regulatory regime for the use and disclosure of credit information', and that 'it would clearly be unsatisfactory to rely solely on generic privacy principles'.[9]

57.14 Stakeholders supported the general proposition that a simplified list of the circumstances in which use and disclosure of credit reporting information is permitted should be set out in the new *Privacy (Credit Reporting Information) Regulations*.[10] Stakeholders approaching the issue from different perspectives recognised, however, that the 'devil would be in the detail'. The Consumer Action Law Centre, for example, stated:

> We would be concerned about any extension of circumstances that allowed access at times other than when the consumer made an application, apart from limited uses in relation to debt collection by the credit provider.[11]

57.15 The Mortgage and Finance Association of Australia stated that, while simplification of the use and disclosure provisions was supported,

> current provisions regarding disclosure to all entities in the distribution chain and the various outsourced service providers are unclear. There should be free exchange of information throughout the distribution chain but only between those entities dealing with a specific borrower and a specific credit.[12]

57.16 The OPC agreed in principle that the regulations should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information, based on those uses and disclosures currently permitted.[13]

57.17 The OPC highlighted the need to consider privacy protection for credit reporting information disclosed by credit reporting agencies and credit providers to specified third parties as permitted by the credit reporting regime—particularly if, as recommended by the ALRC, the regulations are to apply only to personal information

---

9 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

10 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

11 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

12 Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

13 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

maintained by credit reporting agencies or used by credit providers in assessing an individual's credit worthiness.[14] The OPC submitted that the regulations should:

> Apply to the handling of credit reporting information disclosed by credit reporting agencies and credit providers to specified third parties and prohibit the secondary use and disclosure of information held by them.[15]

57.18 In the OPC's view, for example, where a credit provider discloses credit reporting information to a mercantile agent engaged in debt collection, as permitted by s 18N(1)(c), the mercantile agent should be prohibited from using or disclosing that information for secondary purposes.

57.19 The OPC also identified a number of other matters that should be considered as part of the ALRC's review of the existing use and disclosure provisions. It submitted that the ALRC should:

- consider whether the provisions of s 18K ensure an appropriate balance between the needs of law enforcement bodies and the provision of transparency to individuals regarding access by such bodies to their credit reporting information;[16]
- ensure that the use and disclosure of credit reporting information in relation to speech to speech relay services is permitted; and
- determine whether there are other circumstances in which credit providers disclose credit reporting information that should specifically be provided for in the regulations.[17]

Secondary purposes

57.20 Some stakeholders rejected expressly the ALRC's proposal that the new *Privacy (Credit Reporting Information) Regulations* permit use or disclosure of credit reporting information for related secondary purposes on the basis that this would be too permissive.[18] The Australian Privacy Foundation, for example, was of the view that allowing use or disclosure for a related secondary purpose 'defeats the object of more prescriptive credit reporting Rules'.[19]

---

14 See Ch 54, Rec 54–3.
15 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
16 *Privacy Act 1988* (Cth) s 18K(1)(m)–(n).
17 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
18 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.
19 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

57.21 The OPC opposed the proposal, submitting that it was a significant departure from the existing position under Part IIIA without any sound policy justification. The OPC stated that its key concern with the proposal was that

> by design, it would broaden the permitted purposes for which credit information may be used or disclosed beyond what is currently prescribed, to an unknown number of secondary purposes. This would appear to be a significant weakening of existing protections, without clear justification being provided.
>
> Over time, it seems likely that such a mechanism would encourage credit providers and credit reporting agencies to make greater use of credit information for purposes other than the assessment of credit worthiness.[20]

57.22 The OPC submitted that the regulations should, at most, provide that a credit reporting agency or credit provider may use or disclose credit reporting information only for 'directly related secondary purposes (instead of the broader requirement of being a related secondary purpose), to reflect the particular privacy concerns relating to personal credit information'. It also submitted that it should provide guidance on the application of the terms 'directly related' and 'reasonable expectations' in the context of credit reporting.[21]

57.23 Galexia submitted that there should be an express provision prohibiting the collection of credit reporting information from an individual by employers, insurers and government agencies. Galexia added:

> It is also important to note that the economic/public benefit arguments used to justify the special treatment of credit reporting are based on lending dynamics—not employment or other potential applications. If other systems develop that seek access to this type of information they should be consent based and covered by the UPPs.[22]

57.24 Galexia argued that access to credit reporting information should be restricted by a provision in the *Privacy Act* to 'credit providers and organisations that require access to credit reporting information for the management of credit'. This, it was said, would effectively establish a 'tight' primary purpose for collection of credit reporting information.[23]

57.25 The Australian Finance Conference (AFC) considered that the use or disclosure of credit reporting information for secondary purposes should be permitted in accordance with the 'Use and Disclosure' principle. In the AFC's view,

> the secondary use permission contained in UPP 5 is sufficient and a specific regulation is not required. Should a related secondary purpose be identified as a risk

---

20 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
21 Ibid.
22 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.
23 Ibid.

> to consumer credit privacy, then prohibition of use for this purpose should be contained in a Regulation/the Code (eg prohibition against direct marketing).[24]

Credit industry proposal

57.26 The Australasian Retail Credit Association (ARCA) put forward a detailed proposal for reform of the use and disclosure provisions of Part IIIA.[25] This proposal, which was expressly supported by a number of other stakeholders,[26] would significantly liberalise the existing constraints on the handling of credit reporting information.

57.27 ARCA proposed that credit reporting regulations provide for a primary purpose of credit reporting information, and authorise specified secondary use and disclosure of the information. It was suggested that the primary purpose, in relation to the disclosure of credit reporting information to a credit provider, be defined as disclosure:

> for the purpose of making a credit decision affecting an individual and directly related purposes, including the ongoing management and administration of credit and prevention of over commitment, bad debt and identity crime and such other purposes of the credit provider as are specified under the Code.[27]

57.28 ARCA submitted that, in addition to disclosure to credit providers, credit reporting agencies should specifically be authorised to disclose credit reporting information:

- to another credit reporting agency;
- to dispute resolution bodies, where the credit reporting information is relevant to a dispute;
- to a mortgage insurer;
- to a trade insurer;
- to a government body tasked with assisting individuals with credit;
- to a potential assignee of an individual's debt;
- to a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth); and

---

24 Australian Finance Conference, *Submission PR 398*, 7 December 2007.
25 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.
26 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007.
27 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

- as otherwise required by law.[28]

57.29 ARCA and Veda Advantage considered that, in addition, credit reporting agencies and credit providers should be able to rely on a new secondary use provision, measured against the prescribed primary purpose. Veda Advantage suggested that regulation should 'provide for a secondary use mechanism that allows use or disclosure of data that meets the following tests':

- the use is in the reasonable expectation of the consumer
- explicit notice is provided
- a consumer would have consented if consent is possible
- there is benefit for the individual consumer
- there is overall public benefit (including economic efficiency).[29]

ALRC's view

57.30 As noted above, Part IIIA prescribes more than 50 different circumstances in which the use or disclosure of personal information is authorised; and the categories of permitted use and disclosure are exhaustive. It is hard to justify this level of prescription, which risks being overtaken by changes in credit industry practices.

57.31 There is room to simplify and consolidate the use and disclosure provisions of Part IIIA, for example, in relation to use and disclosure by credit reporting agencies and credit providers for the purposes of credit risk assessment;[30] securitisation;[31] or credit assessment of a guarantor.[32]

57.32 A process of consolidation will be necessary, in any case, as a result of the ALRC's recommendation that there should be no equivalent in the new *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*.[33] Some of the circumstances in which the disclosure of information by credit providers is expressly authorised by s 18N may need to be preserved in the regulations, but with application to a more circumscribed category of information.[34]

---

28 Ibid.
29 Veda Advantage, *Submission PR 498*, 20 December 2007.
30 See, *Privacy Act 1988* (Cth) ss 18K(1)(a), 18L(1).
31 See, Ibid ss 18K(1)(ac), 18L(1)(aa)–(ab).
32 See, Ibid ss 18K(1)(c), 18L(1)(b).
33 See Rec 57–6.
34 That is, credit reporting information, rather than personal information related to credit worthiness as defined by s 18N(9)(b).

57.33 The new regulations should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information. This list should be based on the existing provisions of Part IIIA of the *Privacy Act*, subject to the ALRC's other recommendations concerning use and disclosure for specified purposes such as direct marketing and identity verification, discussed below.

57.34 The use and disclosure of credit reporting information is potentially useful for a wide range of secondary purposes. Detailed views on specific use or disclosure of credit reporting information were set out in submissions, including, for example, in relation to mortgage and trade insurance, debt collection, direct marketing and identity verification . These views are discussed in more detail below.

57.35 In DP 72, the ALRC proposed that there be an additional category of permitted use and disclosure of credit reporting information incorporating, expressly or by reference, the secondary use provision in the 'Use and Disclosure' principle in the model UPPs.

57.36 In the light of stakeholder comments and after further consideration, the ALRC considers that the proposal made in DP 72 to permit use and disclosure of credit reporting information for any related secondary purpose within the reasonable expectations of the individual concerned is unjustifiably broad.

57.37 The ALRC's view remains, however, that an additional general category of permitted use and disclosure of credit reporting information should be incorporated into the regulations. Use and disclosure of credit information should be permitted for directly related secondary purposes where the individual concerned would reasonably expect such use or disclosure. The ALRC recommends that, as suggested by a number of stakeholders, this provision refer to the primary purpose of the collection of credit reporting information. This primary purpose should be expressed as 'the assessment of an application for credit or the management of an existing credit account'.

Recommendation 57–1 The new *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information. This list should be based on the provisions of Part IIIA of the *Privacy Act*, which currently authorise the use and disclosure by credit reporting agencies and credit providers of personal information contained in credit information files, credit reports and reports relating to credit worthiness (ss 18L, 18K and 18N).

Recommendation 57–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit reporting agency or credit provider may use or disclose credit reporting information for a secondary purpose related to the assessment of an application for credit or the management of an existing credit account, where the individual concerned would reasonably expect such use or disclosure.

Mortgage and trade insurers

57.38 Part IIIA contains a number of provisions relating to the disclosure of credit reporting information to mortgage and trade insurers;[35] and the use and disclosure of credit reporting information by mortgage and trade insurers.[36] In particular, under s 18K(1)(d) and (e), a credit reporting agency may disclose personal information contained in a credit information file to a mortgage or trade insurer.

57.39 In DP 72, the ALRC asked whether the new regulations should allow credit providers (but not credit reporting agencies) to disclose an individual's credit reporting information to a mortgage or trade insurer, where access to the information is required to assist in the assessment of the individual's credit worthiness.[37]

Submissions and consultations

57.40 The Financial Counsellors Association of Queensland noted:

> It is up to the credit provider to inform insurers of the credit risk of a consumer. Ultimately, it is the credit provider who insists on insurance for riskier consumers. Disclosure should not happen unless the consumer has agreed in writing.[38]

57.41 In addition, a number of stakeholders argued that mortgage or trade insurers only should have indirect access to credit reporting information through the credit provider.[39] The OPC explained current mortgage insurance practices as follows:

> Most credit providers have some discretionary power to approve applications for mortgage insurance. However, where a loan proposal does not meet certain criteria and mortgage insurance is required, for example, where the borrowers are self employed, the mortgage insurer will complete their own assessment of the loan proposal. This involves a complete assessment by the mortgage insurer i.e. they

---

35 *Privacy Act 1988* (Cth) ss 18K(1)(d)–(e), 18N(1)(bb).
36 Ibid 18P.
37 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 53–1.
38 Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.
39 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

> require all the documentary evidence provided to the credit provider such as bank statements and income statements and also request a credit check to complete their assessment.[40]

57.42 The OPC submitted that the new regulations should allow credit providers (but not credit reporting agencies) to disclose an individual's credit reporting information to a mortgage or trade insurer; and require that mortgage and trade insurers use credit reporting information only for the primary purpose for which it was disclosed, and destroy the information once they complete their credit assessment.[41]

57.43 Restricting trade and mortgage insurers to indirect access to credit reporting information was opposed by industry stakeholders.[42] The Insurance Council noted that mortgage insurers are the 'only general insurers who should need access to a borrower's credit history'.[43] The Council observed that, while mortgage insurers have delegated underwriting authority to some of their customers, these delegations are 'limited and strictly controlled'. Further, it submitted that:

> The current credit climate has also seen a significant shift in the market, away from delegation of underwriting authority. Consequently, the Insurance Council considers that the comments of the OPC on this issue are now out of date. Further, some customers who submit applications for mortgage insurance are not credit providers and accordingly do not have access to a credit report. If mortgage insurers did not have direct access to credit report applications when considering mortgage insurance from this class (brokers and originators) then these applications would be delayed pending receipt of a credit report from the credit provider.[44]

57.44 Mortgage insurers provided detailed justifications for maintaining direct access to credit reporting information. They argued that credit reports need to be obtained directly from credit reporting agencies for a number of reasons, including the following:

- Credit reporting information is the only 'truly independent' item of information involved in risk assessment. All other information is 'provided either by the lender, the borrower or an agent of the lender'. To ensure accuracy and to

---

40 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

41 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

42 GE Money Australia, *Submission PR 537*, 21 December 2007; Australian Credit Forum, *Submission PR 492*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; MGIC Australia, *Submission PR 479*, 17 December 2007; PMI Mortgage Insurance Ltd, *Submission PR 412*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

43 Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

44 Ibid.

prevent fraud, it is important that the information comes directly from a credit reporting agency to the mortgage insurer.[45]

- Direct access ensures the timely provision of credit reporting information. This does not disadvantage the individual borrower and permits business-to-business processing of mortgage insurance applications.[46]

ALRC's view

57.45 There is genuine concern that changes to the existing provisions of the *Privacy Act* permitting direct access to credit reporting information by mortgage and trade insures may prejudice existing insurance practices. In view of these concerns, the ALRC is not convinced that there is a sufficiently compelling case to tighten the rules regarding access by mortgage or trade insurers to credit reporting information.

57.46 The new regulations should continue to allow credit reporting agencies to disclose an individual's credit reporting information to a mortgage or trade insurer, where access to the information is required to assist in the assessment of the individual's credit worthiness.

Debt collection

57.47 Credit providers may use credit reports to assist them in recovering overdue payments.[47] A credit provider, in this context, may include a debt collection agency that has purchased debts from a credit provider, or other assignee.

57.48 In addition, a credit provider may disclose certain items of personal information from a credit report to a debt collector for the purpose of collecting overdue payments. The information that may be disclosed is limited to: identifying information about the individual; information about overdue payments; and information about court judgments and bankruptcy orders.[48]

57.49 Where credit providers engaged in debt collection have direct access to the credit reporting system, other issues arise. These include individuals being threatened with having a default listed as a 'collection tool'; the listing of defaults that are disputed by the individuals concerned or without proper notification being given to

---

45 PMI Mortgage Insurance Ltd, *Submission PR 412*, 7 December 2007. See also Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

46 MGIC Australia, *Submission PR 479*, 17 December 2007; PMI Mortgage Insurance Ltd, *Submission PR 412*, 7 December 2007.

47 Section 18K(1)(g) of the *Privacy Act* permits credit reporting agencies to disclose information to credit providers for this purpose.

48 *Privacy Act 1988* (Cth) s 18N(1)(c).

them; and the listing of individuals who are not able to be located as having committed a serious credit infringement.[49]

Submissions and consultations

57.50 Mercantile agents and others engaged in debt collection expressed concern that they are not permitted to obtain personal information on credit information files directly from credit reporting agencies or to report information to agencies. This was said to hamper the ability of mercantile agents to locate debtors and, more generally, to assist small businesses in risk management.[50]

57.51 Some stakeholders highlighted the need for debt collectors to have direct access to the location information available on credit information files, particularly in the light of concerns about restrictions on access to other sources of location information.[51] Others considered that the debt collection provisions were appropriate, and submitted that debt collectors should not be entitled to access credit reporting information directly.[52]

57.52 Veda Advantage acknowledged that 'the threat of default listings as a primary means of, or in the absence of other debt collection activity is of great concern to consumers and their advocates'. Veda considered, however, that such concerns about the use of credit reporting information can be addressed by means other than restricting access—including through credit reporting agency subscription agreements and rules of reciprocity.[53]

57.53 In DP 72, the ALRC stated that there appeared to be no compelling reason for change to the rules restricting access to credit reporting information by debt collectors.[54] The ALRC also noted that many of the debt collection issues raised in submissions are already canvassed in guidance issued by the Australian Competition and Consumer Commission (ACCC) and the Australian Securities and Investments Commission (ASIC), who are jointly responsible for administering consumer protection legislation in relation to the debt collection industry.[55]

---

49 Consumer Credit Legal Centre (NSW) Inc, *Report in Relation to Debt Collection* (2004), 62.

50 Institute of Mercantile Agents and Australian Collectors Association Symposium on Privacy, *Consultation PM 15*, Sydney, 23 November 2006.

51 Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007; EnergyAustralia, *Submission PR 229*, 9 March 2007.

52 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

53 Veda Advantage, *Submission PR 272*, 29 March 2007.

54 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [53.49].

55 Ibid, [53.49] referring to Australian Competition and Consumer Commission and Australian Securities and Investments Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005).

57.54 Some stakeholders agreed with the ALRC's view that the existing position regarding access to credit reporting information by debt collectors should be maintained under the new *Privacy (Credit Reporting Information) Regulations*.[56]

57.55 The Australian Collectors Association submitted, however, that the 'Use and Disclosure' principle in the model UPPs and the new regulations should

> allow creditors, or their collectors and assignees who provide a related secondary purpose, to access a consumer's credit bureau file to seek the most current debtor contact details and debt profile. Alternatively, collectors and assignees could be given the authority to access the credit bureau within a reasonable time after a debt is outsourced for collection or assigned, provided the collector or assignee meets the standards set for other agencies and organisations with bureau access eg membership of an alternative dispute resolution scheme.[57]

57.56 The Australian Collectors Association also noted that debt collectors need 'key customer identification details used within the lending organisation to appropriately identify the customer', and that this information 'is much broader than currently allowed under the Act, which limits information creditors can provide collectors to debtor identity such as name and address and the debt amount'.[58]

ALRC's view

57.57 The use and disclosure of credit reporting information for debt collection purposes is widely accepted as being one of the primary purposes of the credit reporting system. Access to credit reporting information for debt collection is, on some views, essential for the efficient functioning of the credit market.[59] Through the credit reporting system, credit providers share information necessary to locate debtors and are made aware of defaults to other credit providers.

57.58 Concerns about debt collection appear to arise mainly where debt collection activity is outsourced from the original credit provider to debt collection businesses, which may also become the assignees of the debt.[60]

---

56 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Galexia Pty Ltd, *Submission PR 465*, 13 December 2007

57 Australian Collectors Association, *Submission PR 505*, 20 December 2007. The Australian Mercantile Agents Association and the Australian Investigators Association agreed with these views: Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007.

58 Australian Collectors Association, *Submission PR 505*, 20 December 2007. See also Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007.

59 Veda Advantage, *Submission PR 272*, 29 March 2007.

60 Corporations are regarded as credit providers if they acquire the rights of a credit provider with respect to the repayment of a loan (whether by assignment, subrogation or other means): Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006.

57.59 Where debt collectors are not the assignees of the debt, they can only access credit reporting information through the credit provider. This can hinder the debt collection process if the credit provider for whom a debt collector acts is not a subscriber to the credit reporting system. The ALRC understands that part of the reason some organisations have been lobbying for direct access to the credit reporting system is to enable them to service those businesses that, for reasons including size and resources, cannot participate in it directly.

57.60 There is no compelling reason for change to the rules governing access to credit reporting information by debt collectors. The existing barriers to access are not necessarily regulatory. Access may be affected by commercial decisions made by credit reporting agencies in relation to terms and conditions of access, including decisions about fees and the quality of data likely to be provided by potential subscribers.

57.61 Many of the issues raised in submissions are already canvassed in guidance issued by the ACCC and ASIC.[61] For example, the *Debt Collection: Guideline for Collectors and Creditors* reflects the views of the ACCC and ASIC about how provisions of the *Trade Practices Act 1974* (Cth) and *Australian Securities and Investment Commission Act 2001* (Cth) apply to the conduct of debt collection.[62]

57.62 It would not be effective or appropriate for the new *Privacy (Credit Reporting Information) Regulations* to deal with issues that primarily concern debt collection practices. Debt collection practices that involve credit reporting, however, are related to broader concerns about data quality, which are discussed in Chapter 58. For example, consistent reporting of defaults, governed by industry protocols, would lessen the opportunity for debt collectors to threaten listing in order to obtain payment.

Direct marketing

57.63 Direct marketing involves the promotion and sale of goods and services directly to consumers. Credit reporting information is a possible source of personal information from which to generate lists of individuals to whom goods and services may be marketed.

57.64 NPP 2 allows organisations to use personal information for direct marketing with consent or, where it is impracticable for an organisation to seek an individual's consent, the organisation complies with a number of requirements set out in the principle.[63]

---

61 Australian Competition and Consumer Commission and Australian Securities and Investments Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005).

62 Ibid, Guideline 19[g]–[i].

63 The application of privacy principles to direct marketing is discussed in more detail in Ch 26.

57.65 In contrast, Part IIIA does not permit the use or disclosure of personal information for the purpose of direct marketing. Section 18K places limits on the disclosure by a credit reporting agency of personal information contained in an individual's credit information file. The purposes for which such information may be disclosed are set out exhaustively—and disclosure for direct marketing purposes is not among the permitted purposes.

57.66 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* prohibit the use or disclosure of credit reporting information for the purposes of direct marketing.[64]

Submissions and consultations

57.67 There was broad agreement that credit reporting regulation should ensure that credit reporting information is not permitted to be used for direct marketing.[65] ARCA submitted that credit reporting information should 'be precluded from use as a source of direct marketing prospects'. It stated that

> credit providers should be precluded from supplying criteria to a credit reporting agency for the purposes of extracting customer records fitting any particular profile to then solicit business. In addition the credit reporting agencies should be precluded from undertaking such activity, and there should be heavy penalties for any breach of such a rule.[66]

57.68 Those opposed to more comprehensive credit reporting have highlighted concerns that 'such comprehensive, centralised databases may be mined for data by credit providers and other reporting agencies for marketing purposes'.[67] Proponents of more comprehensive credit reporting also emphasised the need to maintain restrictions

---

64 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 53–3.

65 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007; Confidential, *Submission PR 297*, 1 June 2007; American Express, *Submission PR 257*, 16 March 2007; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007. Telstra disagreed, stating that, in this context, 'the need to treat credit information differently from other personal information is unclear': Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

66 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

67 Westpac, *Submission PR 256*, 16 March 2007.

on the use or disclosure of credit reporting information for direct marketing,[68] at least in relation to 'positive' data.[69]

57.69 The Australian Bankers' Association stated that its support for more comprehensive credit reporting was 'strongly predicated on there being effective and enforceable legislative controls on the use of a credit reporting data base for marketing purposes … and severe sanctions for breach'.[70] GE Money Australia, another proponent of more comprehensive reporting, noted that the perceived risk of smaller credit providers or new entrants to the credit marketing 'cherry picking' good customers directly from credit reporting agency lists was one reason for an initial lack of support for more comprehensive reporting in the United Kingdom.[71]

57.70 The Uniform Consumer Credit Code Committee noted that a prohibition on using credit reporting information for direct marketing would be 'consistent with concerns that government fair trading agencies have about unsolicited credit card offers, especially in relation to credit cards and store cards'.[72]

ALRC's view

57.71 The use or disclosure of credit reporting information for the purposes of direct marketing appears inconsistent with the existing provisions of Part IIIA of the *Privacy Act*, which restrict the use and disclosure of such information by reference to an exhaustive list of permitted purposes. Stakeholders expressed strong support for an express prohibition on using credit reporting information for direct marketing.

57.72 Section 18K of the *Privacy Act* does not permit the disclosure of mailing lists derived from credit information files by credit reporting agencies. This position should be maintained under the new *Privacy (Credit Reporting Information) Regulations*. To avoid doubt, the regulations should prohibit expressly the use or disclosure of credit reporting information for direct marketing.

57.73 One model for such a provision is in Hong Kong's *Code of Practice on Consumer Credit Data* (Hong Kong Code).[73] The Hong Kong Code sets out the purposes for which a credit provider may access consumer credit data held by a credit reference agency. It states that:

---

68 Confidential, *Submission PR 297*, 1 June 2007; American Express, *Submission PR 257*, 16 March 2007; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

69 GE Money Australia, *Submission PR 233*, 12 March 2007.

70 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

71 GE Money Australia, *Submission PR 233*, 12 March 2007. For this reason, GE Money favoured a prohibition on the use of 'positive' data in marketing.

72 Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007.

73 Office of the Privacy Commissioner for Personal Data Hong Kong, *Code of Practice on Consumer Credit Data* (1998).

> For the avoidance of doubt … a credit provider is prohibited from accessing the consumer credit data of an individual held by a [credit reference agency] for the purpose of offering or advertising the availability of goods, facilities or services to such individual.[74]

'Pre-screening'

57.74 There was industry support for the idea that, notwithstanding a prohibition on direct marketing, credit providers should be able to use credit reports to 'exclude' individuals from direct marketing offers, for example, to increase credit limits or refinance loans ('pre-screening').[75]

Application of the *Privacy Act*

57.75 While it is clear that Part IIIA of the *Privacy Act* does not permit the use and disclosure of personal information for the purposes of direct marketing, the legal position with regard to pre-screening is more complex.

57.76 The ALRC understands that pre-screening operates as follows. First, a credit provider generates a list of the names of 'prospects' to whom credit may be offered. Such a list may have been generated from the credit provider's own customer lists or may have been acquired elsewhere. The list is then provided to a credit reporting agency, which matches the names on the list with credit information files. Where the credit information relating to an individual is adverse, according to criteria provided by the credit provider, the name is removed from the list. Finally, the 'cleaned' list is provided directly by the credit reporting agency to a mailing house, which sends out an offer prepared by the credit provider.

57.77 In examining the legal position of pre-screening, it is necessary to consider whether the *Privacy Act* permits the:

- disclosure of lists of names and contact details by the credit provider to the credit reporting agency;
- use of the list of names and contact deals in the data-matching process undertaken by the credit reporting agency; and
- disclosure of a 'cleaned' list of names and contact details by the credit reporting agency to the mailing house.

---

74 Ibid, cl 2.12. The Hong Kong Code does not appear to distinguish between direct marketing generally and the pre-screening of direct marketing lists.

75 American Express, *Submission PR 257*, 16 March 2007; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

Disclosure by the credit provider to the credit reporting agency

57.78 Section 18N regulates the disclosure by credit providers of 'reports relating to credit worthiness'. The disclosure of a list of prospective borrowers by a credit provider to a credit reporting agency, however, will not be covered by this provision where the list contains names and contact details only. This is because the list probably does not constitute a 'report', as defined in s 18N(9). In other words, the information it contains does not have 'any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity'.

57.79 Accordingly, the provisions of Part IIIA do not prevent the disclosure of the list for the purposes of pre-screening. The disclosure, however, also must comply with the NPPs. Under NPP 2.1, the disclosure would be permitted if:

- the names and contact details were collected for the primary purpose of direct marketing and disclosure is for this primary purpose; or

- use by the credit provider (that is, in disclosing the list to the credit reporting agency)[76] is for the secondary purpose of direct marketing and the requirements of NPP 2.1(c) have been satisfied.

57.80 The former case might apply where the list was bought from an information broker for direct marketing. In this case, it is arguable that the reason the list is disclosed to the credit reporting agency is clearly to facilitate direct marketing by the credit provider. It is common for organisations who engage in direct marketing to 'clean' lists with personal information from other sources. One interpretation is that the disclosure is, therefore, for the primary purpose of direct marketing and complies with NPP 2.1. Alternatively, it may be argued that disclosure is for the related secondary purpose of checking the credit history of those on the list. If this argument is accepted, the disclosure will breach NPP 2.1(a) unless it is within the reasonable expectation of the individuals concerned.[77]

57.81 Where the list comprises existing customers of the credit provider, it may be possible to argue that the disclosure of the list by the credit provider to the credit reporting agency is for the secondary purpose of direct marketing, and is permitted provided that the requirements of NPP 2.1(c) have been satisfied.

Use of information by the credit reporting agency

57.82 In pre-screening, the credit reporting agency uses personal information contained in its credit information files to 'clean' the personal information contained in the list. That is, a data-matching exercise is undertaken. Part IIIA does not provide

---

76 NPP 2.1(c) refers only to 'use', rather than 'use or disclosure'. As discussed in Ch 26, it is not clear that this has any significance given that 'disclosure' can be cast as 'use'. The 'Direct Marketing' principle in the model UPPs refers to use or disclosure.

77 *Privacy Act 1988* (Cth) NPP 2.1(a)(ii).

limitations on the *use* of credit information files by credit reporting agencies. Rather, s 18K focuses on the *disclosure* of personal information by credit reporting agencies. NPP 2.1, however, generally applies to the use of personal information, including that in credit information files.[78]

57.83 Whether the use of personal information for pre-screening breaches NPP 2.1 depends, first, on a construction of the primary purpose of collection of the information. A narrow construction would be that the information is collected to enable the credit reporting agency to provide a credit report 'to a credit provider who requested the report for the purpose of assessing an application for credit made … to the credit provider'[79] or, more generally, to assess the credit worthiness of individuals. A wider construction would be that the primary purpose of collection is to serve the needs of the credit reporting system. These might include disclosure for any of the purposes permitted under s 18K.

57.84 Whichever construction is taken, the use of the credit information files to pre-screen seems to be a secondary purpose in terms of NPP 2.1(a). This secondary purpose is clearly not related to the primary purpose of assisting a credit provider to assess applications for credit. At the time the list is provided to the credit reporting agency, no application for credit has been made. It is arguable, however, that the secondary purpose is related to a wider construction of the primary purpose—for example, the assessment of credit worthiness.

57.85 In the ALRC's view, the better interpretation is that the use of credit information files by credit reporting agencies for pre-screening direct marketing lists is not permitted by NPP 2.1(a). This interpretation is more consistent with the restrictive and prescriptive provisions of Part IIIA of the *Privacy Act* dealing with the use and disclosure of credit reporting information.

57.86 The use of credit information files by a credit reporting agency to pre-screen lists, however, may be permitted under NPP 2.1(c) if the use of the information by the credit reporting agency can be said to be for the secondary purpose of direct marketing and the other requirements of NPP 2.1(c) have been satisfied.

Disclosure by the credit reporting agency to the mailing house

57.87 Section 18K places limits on the disclosure, by a credit reporting agency, of personal information contained in an individual's credit information file. The purposes for which such information may be disclosed are set out exhaustively in the section. Disclosure to facilitate direct marketing is not such a purpose.

---

78 Except in the case of NPP 2.1(c), which refers only to the 'use', rather than the 'use or disclosure', of personal information for direct marketing.

79 To adopt the words of *Privacy Act 1988* (Cth) s 18K(1)(a).

57.88 The question is whether the disclosure of a pre-screened list by a credit reporting agency to a mailing house constitutes the disclosure of personal information contained in an individual's credit information file in terms of s 18K. From one perspective, all that is being disclosed to the mailing house is a list of names and addresses, which are not derived from the credit information file, but from the list provided by the credit provider. Where the credit information file contains relevant information (that is, showing an adverse credit record) the information is used to delete names from the list. This may distinguish pre-screening from other disclosure of credit reporting information for direct marketing purposes, which is prohibited by s 18K.[80]

57.89 If the 'cleaned' list is returned to the credit provider, rather than to the mailing house directly, there may be an argument that this would constitute a disclosure that breaches s 18K. The absence of some names from the list would be readily apparent and effectively constitutes disclosure that these individuals have the characteristics defined by the credit provider as being sufficient to exclude them from the offer.

57.90 The disclosure of the list by a credit reporting agency to the mailing house is permitted by NPP 2.1 because disclosure is for the primary purpose of collection, that is, for direct marketing purposes.

Conclusions

57.91 The current legal position under the *Privacy Act* with regard to the pre-screening of direct marketing lists is complex. It appears, however, that the use of credit information files by credit reporting agencies to pre-screen lists is not authorised by NPP 2.1(a), as it is not for a secondary purpose related to the primary purpose of collection.

57.92 The credit reporting agency, however, may be able to rely on NPP 2.1(c), which applies only when the use of information is for the secondary purpose of direct marketing. That is, in order to comply with the *Privacy Act*, those engaged in the practice of pre-screening currently must rely on an exception applicable to direct marketing generally. Further, any disclosure of the 'cleaned' list back to the credit provider by the credit reporting agency may breach s 18K.

57.93 The situation under the model UPPs would be similar. The 'Use and Disclosure' principle in the model UPPs follows the wording of NPP 2.1(a) in relevant respects.[81] The ALRC also recommends that the model UPPs contain a separate 'Direct Marketing' principle. This would remove the current distinction, in NPP 2.1(c), between the use or disclosure of personal information for the primary and secondary purpose of direct marketing.[82] It would not, however, significantly change the analysis.

---

80 An alternative analysis is that, in pre-screening, the credit reporting agency acts as an agent of the credit provider.

81 See Ch 25.

82 See Ch 26.

Whether pre-screening complies with privacy principles will still depend on the application of the privacy principles dealing specifically with direct marketing.

Discussion Paper question

57.94 In DP 72, the ALRC asked whether credit providers should be permitted to use credit reporting information to pre-screen and, if so, should credit providers be required to allow individuals to opt out. Alternatively, should credit providers only be permitted to engage in pre-screening if the individual in question has expressly opted in to receiving credit offers.[83]

Submissions and consultations

57.95 Credit reporting agencies and credit providers submitted that credit reporting information should be able to be used for pre-screening.[84] ARCA stated that pre-screening is

> the process by which a credit reporting agency uses credit reporting information to identify individuals with poor credit worthiness and to exclude them from a list provided by a credit provider without disclosure of credit reporting information to the credit provider or another party.[85]

57.96 ARCA submitted that credit providers should be able to use credit reporting information on a 'no-eyes' basis and only using 'negative customer records' (as opposed to more comprehensive credit reporting information). This, it was said, would ensure that pre-screening provides a 'harm reduction outcome' and enhances 'the principle of responsible lending'. ARCA submitted that the definitions used in credit reporting regulation should

> work together to ensure that the use of the centrally held credit information can not be used as a marketing database for the purpose of developing lists for solicitation. It is also not the intention that the information held at each institution about the accounts that their customers hold with them be precluded from use in marketing. The intention is to neither expand nor reduce the personal information available to credit providers from which to develop lists to direct market their products as a result of the introduction of more comprehensive credit reporting.[86]

---

83 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 53–2.

84 Veda Advantage, *Submission PR 498*, 20 December 2007; Westpac, *Submission PR 472*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; American Express, *Submission PR 257*, 16 March 2007; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

85 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

86 Ibid.

57.97 Stakeholders referred to pre-screening as being consistent with responsible lending.[87] Dun and Bradstreet stated that allowing pre-screening would 'be a significant step towards an environment in which unaffordable and unsustainable credit was not offered'.[88] MasterCard noted the importance in the credit card industry of decisions to extend credit limits and submitted that:

> As is current practice, credit report information should be accessible for *excluding* individuals from credit increase offers … It should be noted that this is very different from using credit reports to identify individuals for marketing purposes who should be approached to be offered additional credit. MasterCard opposes the selling of credit information for proactive marketing.[89]

57.98 The AFC stated that, from a public policy perspective, pre-screening 'assists credit providers to offer credit responsibly to individuals and to target their marketing rather than adopting a more-privacy intrusive blanket approach'.[90] Veda Advantage stated:

> All stakeholders agree that it is undesirable for credit to be marketed to individuals who potentially have poor credit worthiness and or are overcommitted. Pre-screening helps achieve that outcome. For an individual consumer whose credit reporting information is used to remove them from a specific direct marketing offer, there is benefit if they are a poor credit risk.[91]

57.99 Veda Advantage noted that mailing houses are required, by contract with the credit reporting agency, to destroy the list after mailing and are prohibited from disclosing the list to any other organisation, including the credit provider.[92] In Veda's view, therefore, the privacy risks involved in pre-screening are 'very slight':

> There is no disclosure of credit reporting information, so there is no additional risk of data breach. If a consumer is wrongly excluded from a marketing list, the outcome is simply that they do not receive a piece of unsolicited marketing information. On the other hand, if a consumer is not removed when they should have been, the outcome is exactly the same as would have occurred if pre-screening were generally prohibited—the consumer receives credit marketing that some might argue they should not.[93]

57.100 Veda Advantage submitted that pre-screening should be permitted only where the individuals concerned are given specific notice that their personal information may be used for pre-screening at the time it is collected; and are given the right to opt out of direct marketing generally.[94] It also noted that further discussions are being held between the industry and consumer and privacy advocates on the related subjects of

---

87 For example, Veda Advantage, *Submission PR 498*, 20 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

88 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232*, 9 March 2007.

89 MasterCard Worldwide, *Submission PR 237*, 13 March 2007.

90 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

91 Veda Advantage, *Submission PR 498*, 20 December 2007.

92 Ibid.

93 Ibid.

94 Ibid. On direct marketing generally, see Ch 26.

pre-screening, direct marketing and responsible lending. In the light of these discussions, Veda requested that the ALRC not make a final recommendation on the position of pre-screening under the new *Privacy (Credit Reporting Information) Regulations*.[95]

57.101 Other stakeholders strongly opposed allowing credit reporting information to be used for pre-screening[96]—primarily on the ground that pre-screening may facilitate more intensive marketing of credit or undesirable credit marketing practices.

57.102 The Consumer Action Law Centre noted that, unless offers are 'pre-approved', an individual always will have to submit a credit application, at which point credit reporting information can be used by a credit provider to assess credit worthiness. A prohibition on pre-screening, therefore, could not 'cause credit to be provided to consumers who have negative information on their credit reports'.[97] The Centre noted that

> rejecting credit applications made by consumers who have received personally addressed invitations to apply, may cause some consumers to be annoyed. Nevertheless, we do not believe that credit reporting information should be used for the purpose of reducing negative impacts that direct marketing may have on the credit provider's image or brand.[98]

57.103 The Consumer Action Law Centre also considered the position of 'pre-approved' (conditionally approved) offers. It noted that rejection of credit applications in response to such offers would pose 'a higher reputational risk for the credit provider'. Pre-screening, therefore, may be 'even more desirable' for credit providers in relation to these offers—particularly when the offers are being made to individuals who are not current customers.[99]

> However, consumer groups such as ours have concerns about the practice of offering 'pre-approved' credit, where from a psychological point of view, consumers seem to be placed in a position of deciding whether to 'reject' credit that is already 'theirs', in circumstances where the consumer has often had no need or desire to obtain credit. We do not support the use of credit reporting information to assist in the making of

---

95 Ibid.

96 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Galexia Pty Ltd, *Submission PR 465*, 13 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.

97 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

98 Ibid.

99 Ibid.

> these offers, or to make the offering of 'pre-approved' credit more attractive to credit providers.[100]

57.104 The Financial Counsellors Association of Queensland submitted that, by allowing pre-screening, 'extra offers of credit could be offered to existing risky consumers' because the financial position of individuals is not subject to proper scrutiny.[101]

57.105 Galexia noted that pre-screening does not necessarily facilitate responsible lending.

> The pre-screened marketing campaigns themselves are often poor examples of responsible conduct. Many of the invitations imply that credit has been pre-approved (some campaigns even include a sample plastic credit card with the target consumer's name embossed on the front of the card). The marketing material contains little information about the risks of credit. Application forms are typically very brief and provide insufficient space for a person to list details of all of their liabilities – they are certainly shorter than the application forms available in branches for the same products.[102]

57.106 The Consumer Action Law Centre and others contested the view that pre-screening reduces the volume of direct marketing of credit.[103] Consumer Action Law Centre stated:

> Pre-screening may reduce the number of offers in a particular campaign, but overall it could actually increase direct marketing of credit, if it makes such campaigns more attractive to credit providers, and therefore leads to more direct marketing campaigns. It may be that some campaigns would not be viable, or would be less viable, without the capacity to screen potential offerees.[104]

57.107 Legal Aid Queensland expressed concern that pre-screening could be used to target particular groups. For example, it was suggested that a credit provider might identify individuals: with housing loans who have a default listed in order to offer refinancing; or with more than two credit cards in order to offer a consolidating loan. Legal Aid Queensland stated that, while it recognised the possible benefit in excluding individuals from direct marking offers, it did not see how pre-screening could be limited in this way.[105] The Consumer Action Law Centre stated that, if pre-screening were to be allowed, it would be essential to define the permitted practices 'very narrowly' because

> 'pre-screening' could be used in a variety of ways, to screen-out various factors, to determine 'pre-approved' limits and to offer differential interest rates—and it could

---

100 Ibid.
101 Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007.
102 Galexia Pty Ltd, *Submission PR 465,* 13 December 2007.
103 Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007.
104 Consumer Action Law Centre, *Submission PR 510,* 21 December 2007.
105 Legal Aid Queensland, *Submission PR 489,* 19 December 2007.

> be used by a larger range of lenders than it is currently (including fringe and sub-prime).[106]

57.108 The Cyberspace Law and Policy Centre observed that allowing pre-screening would 'effectively get round the current limitation that a credit report can only be drawn in relation to an actual application'; and submitted that the wider issue is 'whether unsolicited direct marketing of credit should be allowed and if so under what conditions needs addressing in consumer credit legislation'. It also submitted that 'without compensating lending reforms', pre-screening should be prohibited by the new credit reporting regulations.[107] Similarly, Galexia expressed the view that allowing pre-screening would be contrary to the prohibition on the use of credit reporting information for direct marketing and would send a 'mixed message'.[108]

57.109 While most concern about pre-screening focused on the implications for the marketing of credit, stakeholders also noted the privacy risks associated with the practice. The OPC submitted that pre-screening is 'inconsistent with the policy objective of a robust regulatory scheme for credit information, as well as being inconsistent with community expectations'.[109] Galexia emphasised that pre-screening occurs without the knowledge of the community and could be 'well outside the expectations of the specific consumers whose data is being used in this way'.[110] The Consumer Action Law Centre stated that:

> While the process of pre-screening does not involve credit providers directly accessing individuals' credit reports, we do not believe that this addresses the privacy concerns. Consumers would generally be surprised, and concerned, to find that their personal information was being used in this way.[111]

ALRC's view

57.110 The current legal position under the *Privacy Act* with regard to the pre-screening of direct marketing lists is uncertain. Some stakeholders maintain that neither Part IIIA nor the NPPs prohibit the pre-screening of lists by credit reporting agencies. Conversely, the OPC considers it 'likely that the *Privacy Act* currently prohibits pre-screening of credit offers through the use of the credit reporting system'.[112]

57.111 As discussed above, the legality of the practice depends primarily on whether the credit provider and credit reporting agency are able to rely on the direct marketing

---

106 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.
107 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
108 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.
109 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
110 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.
111 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.
112 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

provisions of the NPPs—and on the use of mailing houses as intermediaries to avoid disclosure of information to the credit provider.[113]

57.112 If pre-screening using credit reporting information were to be permitted, then this would have to be made clear in the new regulations. There are some international precedents for such a course. A report on the international regulation of pre-screening, prepared by Baker & McKenzie for Veda Advantage, identified two jurisdictions—the United States (US) and Ontario, Canada—in which pre-screening is 'impliedly permitted'.[114] In both the US and Ontario, however, the relevant statutory provisions are focused on processes for the 'pre-qualification' or 'pre-approval' of credit, rather than on pre-screening itself.

57.113 In the US, under the *Fair Credit Reporting Act 1970* (US), a consumer reporting agency may furnish a report in connection with a transaction that is not initiated by the consumer if the transaction consists of a 'firm offer' of credit or insurance; and the consumer has not elected to be excluded from pre-screening lists.[115]

57.114 In Ontario, the *Consumer Reporting Act 1990* (Ontario) prohibits the supply of 'a list of names and criteria to a consumer reporting agency in order to obtain an indication of the names of the persons named in the list who meet the criteria' without prior notification of the persons named.[116] This prohibition is subject to an exception where 'a person proposes to extend credit to a consumer'.[117] Under this provision, if direct marketing material given to the consumer informs them that a 'consumer report containing credit information' has been used, the pre-screening exercise is authorised.

Responsible lending

57.115 The possible use and disclosure of credit reporting information in order to pre-screen direct marketing lists presents a range of policy considerations that do not apply to direct marketing more generally. Notably, there is a strong link with consumer protection concerns about responsible lending, the practices of the credit card industry and the direct marketing of credit.

57.116 Industry stakeholders have argued that the ability to pre-screen direct marketing communications assists them in lending responsibly. There is, it is said, a clear commercial and consumer benefit in ensuring that direct marketing of credit products and services is not directed towards those whose applications for credit would, in any case, be refused.

---

113 Galexia referred to the latter practice as a 'technical loophole': Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.

114 Veda Advantage, *Submission PR 498*, 20 December 2007, Attachment 7.2.2, Baker & McKenzie, *International Pre-screening Regulation: An Analysis of the Regulation of 'Pre-screening' by Credit Reporting Agencies in Major Overseas Jurisdictions* (2007), 7.

115 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US), § 1681b(c)(1)(B).

116 *Consumer Reporting Act 1990* (Ontario) s 11(1).

117 Ibid s 10(3).

57.117 From one perspective, permitting pre-screening is consistent with a policy of encouraging or requiring credit providers to assess more fully the financial position of prospective borrowers. On the other hand, pre-screening using credit reporting information could be used as a 'half-measure' in assessing capacity to repay—in substitution for fuller inquiry.

57.118 Consumer groups have expressed concern that pre-screening, by facilitating direct marketing of credit to individuals who have not applied for or expressed an interest in obtaining credit, will result in the granting of excessive amounts of credit. It has been suggested, for example, that pre-screening may encourage the offering of 'pre-approved' loans or increased credit limits.

57.119 The making of unsolicited credit card offers, described as 'pre-approved', has been an issue of significant concern to consumer groups and governments over the last few years.[118] In 2002, the ACT amended the *Fair Trading Act 1992* (ACT) to address concerns about 'pre-approved' credit cards and credit limits.[119] The *Fair Trading Act* now prohibits a credit provider from issuing a credit card, or increasing a credit card limit, unless the credit provider has carried out a 'satisfactory assessment process'.

57.120 A satisfactory assessment process, for these purposes, means

> an assessment of the debtor's financial situation sufficient to satisfy a diligent and prudent credit provider that the debtor has a reasonable ability to repay the amount of credit provided or to be provided.[120]

57.121 It must include asking for (and taking into account), a statement of the debtor's financial situation, including income, all credit accounts and applicable limits and balances, and repayment commitments.[121] To date, no other jurisdiction has followed the example of the ACT.

57.122 The states and territories have sought to maintain harmonisation of consumer credit law through the uniform *Consumer Credit Code*. Issues concerning responsible lending are included on the current Strategic Agenda[122] of the Ministerial Council on

---

118 See, eg, D Tennant, 'Safe and Fair Credit Card Marketing: Why the Credit Industry is So Keen Not to Speak to its Customers' (Paper presented at Consumer Affairs Victoria Credit Law Conference, Melbourne, 8 November 2004); Ministerial Council on Consumer Affairs, *Joint Communiqué: Ministerial Council on Consumer Affairs Meeting*, 18 May 2007.

119 *Fair Trading Act 1992* (ACT) s 28A.

120 Ibid s 28A(3).

121 Ibid s 28A(3)–(4).

122 Ministerial Council on Consumer Affairs, *Ministerial Council on Consumer Affairs: Strategic Agenda* (2007) <www.consumer.gov.au/html/mcca_projects.htm> at 5 May 2008.

Consumer Affairs.[123] After its May 2007 meeting, the Council stated, in a communiqué, that

> Ministers continue to be concerned about the lending practices of credit card issuers in granting excessive amounts of credit to the most vulnerable consumers and look forward to consulting with stakeholders on options for dealing with this issue.[124]

Conclusion

57.123 While pre-screening may be used to assist responsible lending practices, it also has the potential to facilitate more aggressive marketing of credit. As in the case of more comprehensive credit reporting,[125] pre-screening is a tool that may be used by credit providers in different ways and will, as such, not automatically result in more responsible lending practices. To ensure that pre-screening does promote responsible lending would require the enforcement of detailed rules relating to the criteria on which pre-screening may take place.

57.124 It is common ground among stakeholders that using credit reporting information in direct marketing generally should be prohibited. It is artificial to distinguish between 'selecting in' direct marketing prospects (by using credit reporting information to generate a list) and 'selecting out' (by pre-screening an existing list).[126]

57.125 Pre-screening provides clear commercial advantages for credit providers through the better targeting of marketing. One bank observed that 'approval rates following pre-screening for customers applying for credit, can be up to four-fold higher than for non pre-screened data'.[127] Such commercial advantages do not, however, outweigh the privacy and consumer protection concerns raised by pre-screening.

57.126 The new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the use or disclosure of credit reporting information for the purposes of direct marketing, including in relation to the 'pre-screening' of direct marketing lists.

57.127 Credit reporting information includes some publicly available information—such as bankruptcy (personal insolvency) and court judgment information—as well as information from the records of credit providers. The definition of 'credit reporting information'[128] in the new *Privacy (Credit Reporting Information) Regulations* should, however, continue to ensure that publicly available information maintained by a credit reporting agency is covered by credit reporting regulation only where the information is maintained 'in the course of carrying on a credit reporting business'—that is, consumer credit reporting.

---

123 The Ministerial Council on Consumer Affairs consists of all Commonwealth, state, territory and New Zealand ministers responsible for fair trading, consumer protection laws and credit laws.

124 Ministerial Council on Consumer Affairs, *Joint Communiqué: Ministerial Council on Consumer Affairs Meeting*, 18 May 2007.

125 See Ch 55.

126 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

127 ANZ, *Submission PR 467*, 13 December 2007.

128 See Rec 54–3.

57.128 As is presently the case, an organisation should be able to conduct other business undertakings using publicly available or other personal information that it holds, subject to compliance with the UPPs and other obligations under the *Privacy Act*. This might include, for example, using personal information from the National Personal Insolvency Index to pre-screen direct marketing lists.[129]

Recommendation 57–3 The new *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing, including the pre-screening of direct marketing lists.

Identity verification

57.129 Credit providers and other businesses have statutory obligations to verify the identity of their customers, including under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act).[130] One possible source of data for electronic identity verification is credit reporting information held by credit reporting agencies. The use and disclosure of credit reporting information for the purposes of satisfying obligations under the AML/CTF Act was an issue of significant concern to many stakeholders.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

57.130 The AML/CTF Act covers the financial sector, gambling sector, bullion dealers and other professionals or businesses ('reporting entities') that provide particular 'designated services'. The Act imposes a number of obligations on reporting entities when they provide designated services. These include obligations with respect to customer identification and verification of identity, record keeping, establishing and maintaining an AML/CTF program, and ongoing customer due diligence and reporting.

57.131 The customer identification procedures required of reporting entities are set out in Part B of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (the AML/CTF Rules). For example, with respect to individuals and where the money laundering and terrorism financing risk is medium or

129 The National Personal Insolvency Index is established and maintained in accordance with the *Bankruptcy Regulations 1996* (Cth) pt 13.

130 The AML/CTF Act and its relationship with the *Privacy Act* is also discussed in Ch 16. Identity verification may also be required under other legislation such as the *Telecommunications Act 1997* (Cth): see, eg, Australian Communications and Media Authority, *Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*.

lower, the AML/CTF Rules provide for an 'electronic-based safe harbour procedure'.[131]

57.132 In brief, this 'safe harbour' (in terms of compliance with the AML/CTF Rules) is available to reporting entities if they collect the customer's full name; the customer's date of birth; the customer's residential address; and verify:

> (a) the customer's name and the customer's residential address using reliable and independent electronic data from at least two separate data sources; and either
>
> (b) the customer's date of birth using reliable and independent electronic data from at least one data source; or
>
> (c) that the customer has a transaction history for at least the past 3 years.[132]

57.133 The customer identification procedures in the AML/CTF Act supersede identification procedures set out in the *Financial Transaction Reports Act 1988* (Cth). The *Financial Transaction Reports Act* provided prescriptive rules, including the '100 point' identity verification test under which identifying information from various sources is worth a certain number of points.[133] By comparison, the AML/CTF procedures are described as 'risk-based', leaving each institution to make an assessment of the information it needs to gather from its customers.[134]

57.134 Industry stakeholders noted that adopting the 'safe harbour' procedure would be cost-effective because it would streamline the processing of credit applications and eliminate the need for identity verification using physical documents.[135] Electronic identity verification is particularly important for the competitive position of credit providers that do not have branch networks and rely on the internet or brokers to market and distribute their financial products.

> Early adopters of new electronic verification systems, that will allow them to meet their customer identification requirements using online technology, hope to get more out of their investment than a tick from the regulator. They are hoping to win business by making ID checks faster and more convenient and by using the technology to move into new market segments.[136]

---

131 See, *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (Cth) pt 4.2, [4.2.12]–[4.2.13].

132 See, Ibid pt 4.2, [4.2.13].

133 *Financial Transaction Reports Regulations 1990* (Cth) r 4(1). A credit report was worth 35 points under the 100 point identity verification test: *Financial Transaction Reports Regulations 1990* (Cth) r 4(1)(a)(v). Such reports, however, were provided directly to institutions by the individuals concerned, with consent. The ALRC does not propose that the new regulations prevent the disclosure by individuals of their own credit reporting information for identity verification purposes.

134 J Kavanagh, 'ID Checks Create New Market', *The Sheet* (online), 21 December 2007, <www.thesheet .com>.

135 ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

136 J Kavanagh, 'ID Checks Create New Market', *The Sheet* (online), 21 December 2007, <www.thesheet .com>.

57.135 ING Bank summarised the importance of electronic identity verification for reporting entities under the AML/CTF Act:

> - Electronic verification is important to maintain competitive neutrality—This is to ensure that institutions without a branch network have a viable alternative to face-to-face identification.
> - Electronic verification is essential to maintain existing channels for customers to apply for financial services—Electronic banking is a rapidly developing section of the financial services industry ...
> - Electronic verification is cost effective—Electronic verification can streamline the application process, removing the need to deal with customers face to face and allowing for greater efficiency of systems. This is important because it reduces the costs arising from the verification process and means savings can be passed on.
> - Electronic verification provides a robust way of verifying a customer's identity—as it involves conducting verification against the records of a number of independent third parties.[137]

Credit reporting information and identity verification

57.136 Identity verification is a fundamental part of any credit application process. A first step in assessing the eligibility of an individual for credit is to establish the identity of that individual. Other use and disclosure of credit reporting information authorised by Part IIIA—for example, to assess an application for credit, the risk in purchasing a loan by means of a securitisation arrangement or an application for commercial credit—appears to involve the use of credit reporting information in identity verification by a credit provider.

57.137 Sections 18K and 18L of the *Privacy Act*, however, place detailed limits on the disclosure of personal information by credit reporting agencies and the use of personal information by credit providers respectively, and make no express provision for identity verification. Electronic identity verification for the purposes of the AML/CTF Act using credit reporting information is not authorised under Part IIIA because it involves the disclosure of information to reporting entities, as defined in the AML/CTF Act,[138] a category which is much broader than credit providers, as defined by the *Privacy Act*.

57.138 Further, electronic identity verification may be for purposes other than those for which use or disclosure of credit reporting information is authorised—for example, under the AML/CTF Act identity verification may be required in order to accept a

---

137 ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007.

138 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5.

deposit, issue a debit or stored value card, issue a life insurance policy or opening a savings account, or provide a safe deposit box.[139]

57.139 The fact that credit reporting information might be used in electronic identity verification in order to comply with the AML/CTF Act is not sufficient to render disclosure for this purpose by a credit reporting agency 'required or authorised by or under law' for the purposes of Part IIIA.[140]

Discussion Paper question

57.140 The ALRC understands that, in the early stages of planning for the new anti-money laundering legislation, the Australian Government considered a proposal that the Australian Transaction Reports and Analysis Centre would certify third party identity verification services, or direct the establishment of a central source of data for identity verification.[141] The Mortgage and Finance Association of Australia stated that when the AML/CTF legislation was proposed 'it was envisaged that independent electronic means would be available to verify individuals' but that these sources have not become available as envisaged.[142]

57.141 In DP 72, the ALRC considered that it needed more information about the risks and benefits of, and possible alternatives to, the use of credit reporting information in electronic identity verification before making any proposal to address the issue. The ALRC asked, if such use and disclosure were not authorised under the new *Privacy (Credit Reporting Information) Regulations*, what other sources of data might be used by credit providers to satisfy obligations under the AML/CTF Act and similar legislation.[143]

Submissions and consultations

57.142 Industry stakeholders submitted that the new *Privacy (Credit Reporting Information) Regulations* should permit the use and disclosure of credit reporting information for identity verification purposes to satisfy obligations under the AML/CTF Act.[144]

---

139 See definition of 'designated services': Ibid s 6.

140 *Privacy Act 1988* (Cth) s 18K(1)(m).

141 J Kavanagh, 'Credit Files May Provide Identity', *The Sheet* (online), 2 October 2007, <www.thesheet.com>.

142 Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

143 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 53–3.

144 GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Confidential, *Submission PR 517*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007; Abacus–Australian Mutuals, *Submission PR 278*, 10 April 2007; Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007; Experian Asia Pacific, *Submission PR 228*, 9 March 2007.

57.143 Stakeholders emphasised the utility for business and consumers of using credit reporting information for electronic identity verification.[145]

> In order to achieve an appropriate balance between business process efficiency and consumer privacy protection, ANZ is of the view that credit reporting information should be available for the purposes of identity verification for both credit and retail based products. The possibility of using several data sources electronically to create an identity match represents a real benefit, particularly for those businesses where face-to-face interaction with customers is minimal or non-existent. It would also benefit remote customers who do not have access to a bank branch and must use alternative and more onerous methods of providing their identification.[146]

57.144 Veda Advantage submitted that 'electronic verification as a process is considerably less privacy intrusive than documentary based verification' and that the use of personal information in credit reporting 'for identity verification purposes when opening accounts is likely to be well within the reasonable expectations of the consumer'. Veda favoured making specific provision for the use and disclosure of credit reporting information for the purposes of complying with the AML/CTF Act in the *Privacy Act*, as this would make the 'policy intention clear'. Veda also emphasised that the ALRC should not 'pass this issue back to the Government unresolved'.

> The difficulties faced by service providers in efficiently conducting electronic identity verification has significant effect—on the businesses themselves, on the cost of service provision, the end users, the economy, and Australia's competitiveness and international standing. There is an urgent need to have the best datasets for identity verification available. Additional delay or recommendation for further Government review of identity management systems and data is not appropriate.[147]

57.145 Stakeholders noted that credit reporting information is used in comparable jurisdictions for electronic identity verification,[148] and that the use of credit reporting databases has key advantages because they are 'a regulated source, with comprehensive coverage and commercial electronic accessibility'.[149] Other arguments advanced in favour of allowing this use of credit reporting information included that:

- electronic identity verification is essential in promoting greater competition in the banking and financial services market, by ensuring competitive neutrality among financial institutions, removing barriers to entry to the market, reducing

---

145 For example, ANZ, *Submission PR 467*, 13 December 2007; ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

146 ANZ, *Submission PR 467*, 13 December 2007.

147 Veda Advantage, *Submission PR 498*, 20 December 2007.

148 Confidential, *Submission PR 517*, 21 December 2007; ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007. Consumer credit reports are used to verify identity in the US and the United Kingdom: ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007.

149 Confidential, *Submission PR 517*, 21 December 2007; ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007.

regulatory burden and administrative costs and increasing convenience for customers;[150] and

- the Australian Government, having provided for identity verification under the AML/CTF Act, has a 'reciprocal obligation to provide the means for industry to do so' by allowing access to both public and private sector information.[151]

Addressing privacy concerns

57.146 Stakeholders suggested ways to address privacy concerns arising from the use of credit reporting information in electronic identity verification. These included: enacting new restrictions on access to credit reporting information and new penalties for unauthorised access; requiring individual consent to electronic identity verification; limiting the disclosure of credit reporting information to the information needed to verify identity under AML/CTF procedures; ensuring information verified by a credit provider is first obtained from the individual directly; and ensuring that any access for AML/CTF purposes is logged.[152]

57.147 ING Bank proposed that electronic identity verification using credit reporting information should operate with the consent of the individual concerned and the response provided by the credit reporting agency would be

> limited to whether the customer's name, address, date of birth as provided by the reporting entity matches that held by the credit reporting agency, along with the age of the file where a match was found. The response will be in the form of a 'match' or 'no match' response or a single code that represents what has been matched … The reporting entity will not otherwise be able to obtain the name, address or date of birth from the credit reporting agency, nor will it obtain any other information from the credit reporting agency's file (other than age of file for a match).[153]

Other sources of electronic identity verification

57.148 One key consideration in addressing the use and disclosure of credit reporting information for the purposes of the AML/CTF Act is what other sources of data might be used by reporting entities for electronic identity verification.

57.149 ING Bank provided a comprehensive survey of the possible alternative sources of data for electronic identity verification. These included sources of data held

---

150 Confidential, *Submission PR 517*, 21 December 2007.
151 Optus, *Submission PR 532*, 21 December 2007.
152 Confidential, *Submission PR 517*, 21 December 2007; ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007.
153 ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007.

by the Australian Government,[154] state and territory government,[155] and the private sector.[156] In conclusion, ING Bank stated that it had been

> unable to identify any comprehensive data sources for date of birth that are able to support high volume, real-time electronic response. As a result, industry cannot utilise the electronic verification safe harbour provisions in the AML/CTF Rules.[157]

57.150 In DP 72, the ALRC referred to the Australian Government's Document Verification Service (DVS).[158] The DVS enables an agency to verify that a document, which is presented to the agency by an individual to prove his or her identity, was issued by the document issuing agency claimed on the face of the document.[159]

57.151 ING Bank noted that the DVS is premised on the reporting entity first obtaining the physical identification documents from the customer, then utilising the service to verify the authenticity of the documents against government databases.

> This will still be reliant on the customer sending in identification documentation, therefore it will not support online electronic verification and also does not remove the risk of sensitive documents being lost or intercepted via mail where the customer opts for the convenience of a non face to face channel.[160]

57.152 The AFC observed that, while there are some electronic databases, including the electoral roll and telephone directories, that are currently accessible to verify name and residential address, there are 'few, if any, avenues of easily and efficiently verifying a transaction history by e-means'.[161]

57.153 There are also inadequacies in the available date of birth information. The AFC advised that the 'only data source currently available to our financier members to validate date of birth' is the state-based Certificate Validation Service (CVS), based on data from state and territory registers of births, deaths and marriages.

> While the CVS has been useful in terms of AML/CTF compliance it has a number of limitations which put at issue its 'reliability'. For example, the CVS requires input of

---

154 For example, held by the Australian Electoral Commission (electoral roll); the Department of Foreign Affairs and Trade (relating to resident non-citizens) and ASIC.

155 For example, registries of births, deaths and marriages and motor vehicle registries.

156 For example, the Telstra Integrated Public Number Database.

157 ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007.

158 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [53.86].

159 Australian Government Attorney-General's Department, *Identity Security—National Document Verification Service (DVS)* <www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity> at 5 May 2008.

160 ING Bank (Australia) Limited, *Submission PR 420*, 7 December 2007. ING Bank also noted that 'there has been no clear timetable for delivering DVS and access by commercial organisations has also not been confirmed nor assessed for suitability'.

161 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

> a certificate or registration number which a customer is unlikely to carry in their wallet as they would a driver's license.[162]

57.154 The AFC noted that its members are more likely to use electronic identity verification products offered by an information broker (for example, Veda Advantage or FCS OnLine) than develop a system for themselves.[163]

57.155 Some stakeholders with an interest in providing electronic identity verification services questioned the suitability and reliability of credit reporting information for this purpose. The Global Data Company stated that credit reporting information may require some form of 'washing' or further verification before it can be used for identity verification purposes; and noted that it is not held or administered by a government agency. Further,

> if credit reporting information is to be used for identity verification purposes, it must be available to Reporting Entities, or service providers to Reporting Entities, on a relatively free and fair basis. Given that such information is currently held exclusively by private entities with a pecuniary interest in maintaining some degree of control and monopoly over the data, it is unlikely that this fundamental requirement could be achieved. The possibility that certain commercial entities could enjoy a massive financial windfall purely as a consequence of being able to utilise individuals' personal data (which was collected for an entirely unrelated purpose) is fundamentally inconsistent with any proper implementation of the principles underpinning the AML/CTF Act.[164]

57.156 FCS OnLine stated that the use of credit reporting information in electronic identity verification is inappropriate

> as its collection and verification is subject to no publicly known quality control checks. The information is apparently secondary in nature, compiled from indeterminate sources, and would never have been completely verified against an authoritative government database (as there has not been any available—eg for DOB information).[165]

57.157 These stakeholders emphasised the availability of alternative sources of data, if existing restrictions on access to this data were lifted. The Global Data Company submitted that providing additional sources of date of birth information would be preferable to permitting access to credit reporting information for electronic identity verification.

> First, date of birth information is likely to be more reliable and independent because it would originate from a legitimate government source … Second, date of birth information is static, in contrast to credit reporting information which necessarily

---

162 Ibid. In addition, the CVS does not cover individuals born in either Tasmania or the Northern Territory and coverage is limited by date of birth in other jurisdictions (eg, for individuals born in Western Australia, the data is only available for those born after 1974): Australian Finance Conference, *Submission PR 398*, 7 December 2007.

163 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

164 Global Data Company, *Submission PR 409*, 7 December 2007.

165 FCS OnLine, *Submission PR 441*, 10 December 2007.

> requires ongoing update. Third, access to date of birth information can be easily arranged given that it can be obtained from the Electoral Roll (which is already a current source of name and address information).[166]

57.158 The Global Data Company observed that

> it is currently not possible to access date of birth information on individuals in Australia, notwithstanding that such data is collected and stored by a multitude of state and federal government agencies. This is puzzling given the fact that the AML/CTF Rules explicitly contemplate such data as a source for identity verification purposes.[167]

Opposition to use or disclosure for electronic identity verification

57.159 A number of stakeholders opposed the use or disclosure of credit reporting information for electronic identity verification,[168] or considered that any proposal to permit such use or disclosure would be premature, or inappropriate in the context of a privacy review.[169]

57.160 The Cyberspace Law and Policy Centre noted that, despite many submissions on the issue, 'the previous government chose not to accommodate any relaxation of or exemption from the *Privacy Act*' in relation to the AML/CTF Act. The Centre submitted that:

> The ALRC should not take a position in relation to wider use of credit reporting information for identity verification outside the context of credit assessment, other than to recommend that it be considered in the context of wider identity management strategies.[170]

57.161 The Australian Privacy Foundation opposed the use of credit reporting information for the purposes of the AML/CTF Act and stated that, given the Australian Government's previous decision not to provide for reporting entities to have access to credit reporting information, changes to the *Privacy Act* should not be made to allow for 'back door' access by credit providers.[171]

57.162 The OPC stated that the credit reporting system should not be subject to expanded uses and disclosures that are unrelated to the reason for which credit reporting information was originally collected—namely, the assessment of individuals' eligibility for credit. The OPC reiterated that the use of credit reporting information for electronic identity verification would be 'inconsistent with the original intent of

---

166 Global Data Company, *Submission PR 409*, 7 December 2007.
167 Ibid.
168 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; Min-it Software, *Submission PR 236*, 13 March 2007.
169 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
170 Ibid.
171 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

Parliament and it would represent a substantial change in terms of individuals' expectations about how credit information would be used and to whom it would be disclosed'.[172]

57.163 The OPC submitted that proposals to expand the use of the credit reporting system in this way should be the subject of a separate review by the Australian Government. As part of this review, the OPC suggested the following matters be considered:

- the breadth of organisations that would have access to the credit reporting system for electronic identity verification purposes;
- what information would be used and disclosed for identity verification purposes;
- what limitations would be in place regarding secondary use and disclosure of this information;
- how privacy protections such as openness, consent and accuracy would be complied with under such a proposal.[173]

ALRC's view

57.164 The AML/CTF Act imposes obligations on reporting entities with respect to customer identification and verification of identity. In some circumstances, the procedures prescribed by the AML/CTF Rules allow for electronic identity verification, which has a range of advantages for reporting entities. Stakeholders have expressed concern that they are not authorised to obtain electronic data, including credit reporting information, that would enable them to use electronic identity verification effectively.

57.165 The AML/CTF Rules provide flexibility with regard to the means of identity verification. As noted above, verification of information collected about a customer may be based on: reliable and independent documentation; reliable and independent electronic data; or a combination of these.[174]

57.166 A range of sources of information could potentially be used for electronic identity verification. These sources include those that are currently available, such as the electoral roll and registers maintained by ASIC; and those to which access is restricted by regulation or administrative practice, such as credit reporting information, the Integrated Public Number Database maintained by Telstra; and state and territory registries of births, death and marriages.

---

172 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
173 Ibid.
174 *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (Cth) [4.2.7].

57.167 There are arguments in favour of allowing credit reporting information to be used and disclosed for electronic identity verification. These include that credit reporting information comes from a regulated source with relatively comprehensive coverage, it is easily accessible electronically, and it is an important source of date of birth information.[175]

57.168 The use and disclosure of credit reporting information for electronic identity verification cannot be considered in isolation. Other data sources and the broader identity management strategies of government and private sector bodies must also be considered. Arguments may be advanced in favour of allowing the use and disclosure of personal information from other data sources in preference, or in addition, to credit reporting information. For example, while the *Commonwealth Electoral Act 1918* (Cth) allows the Electoral Commission to provide reporting entities with the names and addresses of individuals on the electoral roll,[176] it prohibits disclosure of individuals' occupations, sex or date of birth.[177] Consideration could be given to allowing the Australian Electoral Commission to provide reporting entities with date of birth information, which might reduce the need to use credit reporting information.

57.169 The OPC submitted that the question of access to credit reporting information for AML/CTF identity verification should be examined through a separate consultative process that considers the potential benefits and risks of the proposal in greater detail.[178] In Chapter 16, the ALRC recommends that the statutory review of the AML/CTF regime[179] should consider a number of matters, including whether the use of the electoral roll by reporting entities for the purposes of identification verification is appropriate.[180] While the use of credit reporting information for electronic identity verification could be left for consideration as part of that review, the review does not have to be conducted until 2013.

57.170 There was opportunity to provide specific authorisation for the use of credit reporting information during the legislative process that led to the enactment of the AML/CTF Act and the issuing of the AML/CTF Rules, but this was not done. Rather, the ALRC understands that the Government deferred consideration of the use and disclosure of credit reporting information for identity verification until after the completion of this Inquiry. In these circumstances, the ALRC considers that it must reach a concluded view on the question.

---

175 One possible limitation of credit reporting information as a source of 'independent' electronic data, however, is that credit reporting information used by a reporting entity to verify identity may have come from the same reporting entity in the first place—because credit reporting agencies aggregate information provided by their credit provider members.

176 *Commonwealth Electoral Act 1918* (Cth) s 90B(4), items 6 and 7.

177 Ibid s 90B(7).

178 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

179 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 251.

180 See Rec 16–4.

57.171 On balance, the ALRC considers that, while the use and disclosure of credit reporting information for electronic identity verification would constitute a significant 'function creep', it should be authorised specifically under the AML/CTF Act. The reasons for this view include that:

- electronic identity verification provides significant advantages for both credit providers and individuals;
- electronic identity verification is less privacy intrusive than the need to present physical records to verify identity; and
- there are limited alternative sources of accessible data suitable for electronic identity verification.

57.172 Following amendment of the AML/CTF Act, the use and disclosure of credit reporting information would be 'required or authorised by or under law' for the purposes of the new *Privacy (Credit Reporting Information) Regulations*. It would, therefore, fall within the list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information.

57.173 The ALRC notes that, before this recommendation can be implemented a wide range of issues require further consideration. These include whether: legislation should prohibit the secondary use or disclosure by reporting entities of credit reporting information obtained for identity verification purposes; reporting entities should have positive obligations to seek consent from individuals before using credit reporting information to verify identity; and reporting entities should be required to have processes in place to resolve mismatches between the information individuals provide and credit reporting information.[181]

57.174 An alternative approach would be to authorise the use and disclosure of credit reporting information for electronic identity verification in the new *Privacy (Credit Reporting Information) Regulations*. This would replicate, in broad terms, the approach taken by the *Commonwealth Electoral Act*, which provides for the disclosure of electoral information to reporting entities.[182]

57.175 In the ALRC's view, however, this would introduce undesirable complexity into the new *Privacy (Credit Reporting Information) Regulations*, given the need for additional provisions dealing with the specific categories of credit reporting information that may be disclosed, and with the other matters referred to above. Further, the use or disclosure of personal information for the purposes of the AML/CTF Act is broadly for law enforcement purposes—namely, to combat money laundering and the financing of terrorism. It is not the approach of the *Privacy Act* to

---

181 As suggested by the OPC: Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

182 *Commonwealth Electoral Act 1918* (Cth) s 90B, items 6 and 7.

provide expressly for such exceptions, but to deal with them under the general 'required or authorised by or under law' exception (or through exemptions for law enforcement agencies).

Recommendation 57–4 The use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) should be authorised expressly under the AML/CTF Act.

Identity theft

57.176 In this Inquiry, the ALRC examined whether credit reporting regulation should provide expressly for the problem of identity theft—the theft or assumption by a person of the pre-existing identity of another person.[183] For example, credit reports might be permitted to contain information that the individual concerned has been the subject of identity theft.[184]

57.177 In the US, under the *Fair Credit Reporting Act 1970* (US), an individual may, in defined circumstances, require that a credit reporting agency insert a 'fraud alert' on a credit information file. A fraud alert is a statement that notifies prospective users of a credit report that the individual concerned 'may be a victim of fraud, including identity theft'.[185] Credit reports in the United Kingdom are also permitted to indicate that the individual has been the subject of identity theft.[186] Some stakeholders supported the suggestion that similar provisions be implemented in Australia.[187]

57.178 In some jurisdictions,[188] legislation allows for a court certificate to be issued to a victim of identity crime[189]—on the court's own initiative or on application by either

183 See Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006), 15.

184 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–23.

185 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US) § 1681c–1.

186 Experian Asia Pacific, *Submission PR 228*, 9 March 2007.

187 Australian Finance Conference, *Submission PR 294*, 18 May 2007; Queensland Law Society, *Submission PR 286*, 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007; Min-it Software, *Submission PR 236*, 13 March 2007; Experian Asia Pacific, *Submission PR 228*, 9 March 2007; Australian Institute of Credit Management, *Submission PR 224*, 9 March 2007.

188 *Criminal Law (Sentencing) Act 1988* (SA) s 54; *Criminal Code* (Qld) s 408D.

189 Australian Finance Conference, *Submission PR 294*, 18 May 2007.

the victim or the prosecutor. Such certificates do not compel others to take action—for example, to correct an individual's credit reporting information—but provide 'a means to present the outcome of a court's decision in a way that may be used by the victim'.[190] One such use might be to substantiate an individual's claim to have been the subject of identity theft. The Australian Government has proposed that all jurisdictions be empowered to 'issue certificates to victims of identity crime to help them establish their credit histories'.[191]

57.179 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should provide for the recording, on the initiative of the relevant individual, of information that the individual has been the subject of identity theft.[192]

Submissions and consultations

57.180 This proposal received support, at least in principle, from industry and consumer stakeholders.[193] Questions were raised, however, about what evidence of identity theft should be required in order for a notation to be made.[194] It was also suggested that credit providers should be under some obligation to list identity theft information and to notify the individual about it.[195]

57.181 Stakeholders confirmed that making notations may have limited practical effect where credit reporting information is processed electronically.[196] Veda Advantage noted:

> Almost no credit provider ever sees a physical credit report. Rather, credit reporting information is provided as a data stream to a credit provider, which normally processes it in an automated system.[197]

---

190 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Discussion Paper—Identity Crime* (2007), 28.

191 T Allard, 'New Laws to Fight Identity Theft', *Sydney Morning Herald* (Sydney), 27 March 2008, 3.

192 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–1.

193 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Credit Forum, *Submission PR 492*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

194 Australian Credit Forum, *Submission PR 492*, 19 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

195 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

196 Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

197 Veda Advantage, *Submission PR 498*, 20 December 2007.

57.182 For this reason, Veda Advantage stated that providing for the recording of information about identity theft would be ineffective. A number of stakeholders, including Veda, considered that permitting an individual to put a 'freeze' on credit reporting information would be a better way to address concerns about identity theft.[198] Such a mechanism would allow an individual to make his or her credit reporting information inaccessible to any credit provider, making it more difficult for anyone to open a credit account in the individual's name.

57.183 In the US, 39 states and the District of Columbia have enacted laws requiring credit reporting agencies to enable individuals to protect their credit files with a security freeze. In addition, the major credit reporting agencies offer such a mechanism voluntarily in the states that have not yet adopted security freeze laws.[199] The US Federal Trade Commission is considering whether a federal security freeze law would be appropriate.[200]

57.184 ARCA stated that in Australia the security freeze mechanism should 'allow a consumer who fears they have been subject of identity theft to freeze and unfreeze their credit file at their request, preventing fraudsters obtaining access to credit', and suggested that the issue should be dealt with in the credit reporting code.[201]

57.185 National Legal Aid supported the introduction of a security freeze mechanism, provided that 'credit providers who do not access the credit report before assessing an application for credit should not be able to list a default, if the account has been frozen and they are unable to prove that the debt was incurred by the named debtor'.[202] Similarly, Legal Aid Queensland stated that a freeze would be a 'good solution' but that it

> does not deal with credit providers who do not check credit reports prior to extending credit, but only use reports to report default information. If the ALRC accepted the industry's recommendation that consumers could freeze the account to prevent fraud then we propose that any creditor who extends credit during the freeze, should not be able to default list.[203]

---

198 GE Money Australia, *Submission PR 537*, 21 December 2007; Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

199 Consumers Union, *Consumers Union's Guide to Security Freeze Protection* (2007) <www.consumersunion.org/campaigns/learn_more/003484indiv.html> at 5 May 2008.

200 United States Federal Trade Commission, *Prepared Statement Before the Maryland Task Force to Study Identity Theft* (2007).

201 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

202 National Legal Aid, *Submission PR 521*, 21 December 2007.

203 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

57.186 Dun and Bradstreet considered that reform should not be limited to implementing a freeze mechanism because this would create a 'burden for consumers to unfreeze'.[204] The Cyberspace Law and Policy Centre stated:

> We would need to see more detail of this proposal before forming a view as to whether it is an adequate substitute for a flag that can (and in our view) should be taken into account while the file continues to be in use. The extent to which it is appropriate for the file to remain in use will depend on the type of crime and stage of response to it.[205]

ALRC's view

57.187 There is concern that identity theft is becoming more prevalent due to developments in information and communications technology.[206] The idea that individuals should have the right to prohibit the disclosure by a credit reporting agency of credit reporting information about them without their express authorisation (that is, to 'freeze' disclosure) received significant support from both consumer and industry stakeholders. The ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should provide for such a right.

57.188 Providing for notations in credit reporting information that the individual has been the subject of identity theft[207] may not achieve the desired result for the individuals concerned. The first problem is that such notations may have no effect where credit reporting information is processed electronically. Secondly, even where seen by a credit provider, it is unclear what the practical effect of such a notation would be. While it may be expected that the credit application would be declined—at least until further inquiries are undertaken by the credit provider—this may not necessarily be the case. In contrast, the right to freeze the disclosure of credit reporting information recommended by the ALRC should prevent credit being advanced.

57.189 The ALRC agrees that, in addition, a credit provider that advances credit during the period an individual has frozen his or her credit reporting information should not be able to list information—and, in particular, default information—concerning that credit, except with the consent of the individual.

Recommendation 57–5 The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to prohibit for a specified period the disclosure by a credit reporting agency of credit reporting information about them without their express authorisation.

---

204 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007.
205 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
206 See Ch 12.
207 As proposed in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 52–1.

Disclosure of reports relating to credit worthiness

57.190 Section 18N applies to information contained in 'reports relating to credit worthiness'.[208] Section 18N(9) provides that a 'report' is defined, for the purposes of the section, as:

> (a) a credit report; or
>
> (b) … any other record or information, whether in a written, oral or other form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity;
>
> but does not include a credit report or any other record or information in which the only personal information relating to individuals is publicly available information.[209]

57.191 Consequently, s 18N(9) protects a broader category of information than other provisions of Part IIIA, which protect information contained in a 'credit report' or 'credit information file'. For example, while the disclosure by a credit provider of this broader category of information is protected,[210] credit providers' obligations to ensure the accuracy and security of information under s 18G apply only to information in a credit report—that is, information provided by a credit reporting agency.

57.192 In effect, s 18N creates a comprehensive regime with regard to the disclosure by credit providers of personal information that may have no connection with the credit reporting system. The section applies to personal information that has 'any bearing' on an individual's credit worthiness, credit standing, credit history or credit capacity. This category of information seems broad enough to include information about, for example, an individual's income, expenditure and employment and even his or her family or school connections.

57.193 The reach of s 18N is anomalous within Part IIIA, which otherwise applies only to personal information in 'credit information files' or 'credit reports' as those terms are defined in s 6(1).[211]

57.194 In DP 72,[212] the ALRC noted that the second reading speech for the Bill that introduced the credit reporting provisions[213] indicated that the purpose of the Bill was to establish a privacy framework for the regulation of the 'consumer credit reporting industry'.[214] There was no reference to the establishment of a regime regulating the

---

208 Section 18N is described in detail in Ch 53.

209 *Privacy Act 1988* (Cth) s 18N(9).

210 See, eg, *F v Credit Provider* [2003] PrivCmrA 4, where a store breached s 18N by informing a customer's former partner that her account with the store was in arrears.

211 With the exception of *Privacy Act 1988* (Cth) s 18Q, which applies to information obtained from credit providers by certain persons.

212 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [53.92].

213 Privacy Amendment Bill 1989 (Cth).

214 See, eg, Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

disclosure of all credit worthiness information held by credit providers.[215] This resulted from the insertion of an extended definition of 'report' following amendments to the Bill in 1990.

Discussion Paper proposal

57.195 In DP 72, the ALRC proposed that there should be no equivalent of s 18N of the *Privacy Act* in the new *Privacy (Credit Reporting Information) Regulations*.[216] The ALRC expressed the preliminary view that the use and disclosure limitations in the regulations should apply only to personal information maintained by credit reporting agencies and used in credit reporting—that is, to 'credit reporting information' as defined in the regulations.

Submissions and consultations

57.196 There was significant support from industry stakeholders for the ALRC's proposal.[217] Telstra, for example, stated that it supported the abolition of the s 18N restrictions

> on the basis that the new UPPs should provide adequate protection to the information currently covered by the definition of 'report'. Telstra does not understand the policy reasons behind section 18N (or any new equivalent) imposing additional restrictions to the NPPs in relation to information other than credit reports.[218]

57.197 Other stakeholders considered that an equivalent of s 18N of the *Privacy Act* should be included and that the new regulations should apply to the broader category of information encompassed by s 18N(9).[219]

57.198 The Cyberspace Law and Policy Centre stated that, notwithstanding the subsequent enactment of privacy principles applying to personal information held by organisations generally, 'the arguments for more specific regulation of credit related personal information ... apply with equal force to both credit reporting information and credit reports as defined in s 18N'.[220] The Centre also noted that, while the scope of s 18N may not be well-known (or observed) by credit providers,[221] 'this is an argument

---

215 The Cyberspace Law and Policy Centre noted, however, that the Second Reading Speech also stated that the principal purpose of the Bill was to provide privacy protection for individuals in relation to their 'consumer credit records': Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

216 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 50–5.

217 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

218 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

219 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

220 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

221 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [53.96].

for greater education and enforcement activity, not for abandoning the regulation, without a more convincing case'.[222]

57.199 The OPC submitted that a term 'credit worthiness information' should be defined separately from 'credit reporting information' in the new regulations and that the definition should be based, in part, on the definition of 'report' in s 18N(9)(b). Further, it submitted that the new regulations should place limits on the use and disclosure of 'credit worthiness information' by credit providers. The OPC suggested that explanatory statements to the new regulations provide guidance on what types of personal information are included within the term 'credit worthiness information', and expressed a willingness to provide additional guidance on this question.[223]

ALRC's view

57.200 The ALRC remains unconvinced that there is any good reason to retain an equivalent of s 18N in the new *Privacy (Credit Reporting Information) Regulations*. The extended reach of s 18N can be understood as eventuating because Part IIIA was enacted before the NPPs. Section 18N was needed to ensure there was no way to avoid the application of the new credit reporting provisions by, for example, disclosure between credit providers directly, without the intermediary of a credit reporting agency. This rationale no longer applies.

57.201 The breadth of the information covered by s 18N means that there is an enormous overlap with the coverage of the NPPs. Information that 'has any bearing on an individual's credit worthiness' in terms of s 18N(9)(b) could include information about an individual's attitudes, assets, income or even family connections. The handling of personal information relating to credit worthiness that has no relationship with credit reporting agencies should be regulated by general privacy principles and not by the new *Privacy (Credit Reporting Information) Regulations*.

57.202 The ALRC is not aware of any other jurisdiction that in this way regulates personal information relating to credit worthiness. In New Zealand, for example, the *Credit Reporting Privacy Code 2004* (NZ) regulates the use and disclosure of 'credit information' by 'credit reporters' and the definition of credit information is limited to the information that credit reporters are permitted to collect.

57.203 In Chapter 54, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should apply only to information that is maintained by a credit reporting agency; or held by a credit provider, having been prepared by a credit reporting agency, and used in establishing an individual's eligibility for credit.[224]

---

222 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
223 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
224 Rec 54–3.

Consistently, there should be no equivalent in the *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act.*

Recommendation 57–6 There should be no equivalent in the new *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information in 'reports' related to credit worthiness. The use and disclosure limitations should apply only to 'credit reporting information' as defined for the purposes of the new regulations.

58. Data Quality and Security

Contents

Introduction

58.1 This chapter discusses the existing provisions of Part IIIA of the *Privacy Act 1988* (Cth) dealing with the data quality and security of credit reporting information and makes recommendations on how these matters should be dealt with under the

model Unified Privacy Principles (UPPs)[1] and the new *Privacy (Credit Reporting Information) Regulations*.

Data quality and credit reporting information

58.2 The 'Data Quality' principle in the model UPPs provides that:

> An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

58.3 Section 18G(a) of the *Privacy Act* provides that credit providers and credit reporting agencies have an obligation to take reasonable steps to ensure that personal information in a credit information file or credit report is 'accurate, up-to-date, complete and not misleading'. In addition, the *Credit Reporting Code of Conduct* provides for the steps to be taken by a credit reporting agency when it becomes aware that information supplied by a credit provider may be inaccurate. If the agency believes that other credit information files may contain similar inaccurate listings it must, as soon as practicable, notify the credit provider and request the credit provider to investigate the accuracy of other files that may be similarly affected.[2]

58.4 The quality of credit reporting information is of fundamental importance to individuals, given the significant consequences that may flow, in terms of future access to credit, from an adverse credit report. Data quality, in the context of credit reporting, has a number of important aspects.

- Credit reporting information may be inaccurate because the individual has been identified incorrectly (that is, cases of mistaken identity); or information may be 'about' the correct individual, but inaccurate for other reasons.

- Credit reporting information may be accurate in objective terms, but not comply with regulatory standards relating to data quality, such as those prescribing the permitted content of credit information files.[3]

- The consistency of data reported by credit providers is an important aspect of data quality, because if the same information is reported inconsistently, it may be misinterpreted more easily.

- Overdue payment information may be considered inaccurate because: the debt to which the payment relates is disputed; information relating to the same debt has been reported multiple times; or the debt has been paid but repayment has not been recorded.

---

1 See Part D.
2 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [1.4].
3 *Privacy Act 1988* (Cth) s 18E.

Regulating data quality

58.5 The 'Data Quality' principle in the model UPPs and the data quality obligations in Part IIIA[4] are similar. The 'Data Quality' principle, therefore, may be considered adequate to cover credit reporting information without the need for separate provisions in the new *Privacy (Credit Reporting Information) Regulations.*

58.6 There are, however, some important differences between the obligations in the UPPs and in Part IIIA. These are that:

- section 18G(a) provides an additional requirement that personal information be 'not misleading'; and
- the 'Data Quality' principle provides an additional requirement that personal information be 'relevant'.[5]

Discussion Paper proposal

58.7 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC expressed the view that the existing formulation of the data quality obligation set out in s 18G(a) should be retained for the purposes of credit reporting regulation. It proposed that the new *Privacy (Credit Reporting Information) Regulations* provide that credit providers and credit reporting agencies have an obligation to take reasonable steps to ensure that credit reporting information is accurate, up-to-date, complete and not misleading.[6]

Submissions and consultations

58.8 Stakeholders generally supported the imposition of data quality obligations in the new regulations, as proposed by the ALRC.[7] The Office of the Privacy Commissioner (OPC) submitted, however, that the relevance requirement in the 'Data Quality' principle should be 'retained and strengthened' in relation to credit reporting.[8] The Cyberspace Law and Policy Centre and the Australian Privacy Foundation also stated that the regulations should include the relevance requirement, to be as consistent

---

4 Ibid s 18G(a).

5 The reasons for the formulation preferred in the model UPPs are set out in Ch 27.

6 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 54–4.

7 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

8 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

as possible with the 'Data Quality' principle.[9] Conversely, Veda Advantage submitted that the requirement of relevance is not within the control of credit reporting agencies and, therefore, should not be part of credit reporting data quality obligations.[10]

58.9 The OPC suggested that it provide guidance for credit providers and credit reporting agencies about what measures are considered to be 'reasonable steps' to promote and maintain the accuracy of credit reporting information.[11]

ALRC's view

58.10 The major discrepancy between the criteria set out in the 'Data Quality' principle and in s 18G(a) is the additional requirement in s 18G(a) that information be 'not misleading'. In DP 72, the ALRC stated that, in the credit reporting context, information may be 'accurate' but misleading in relation to the credit worthiness of an individual. This may be, for example, due to circumstances surrounding a default listing, such as a billing failure on the part of the credit provider.[12] On the other hand, in most situations where information fails to meet the requirement of 'not misleading', it also will not meet the requirements that it must be 'accurate', 'complete' or 'up-to-date'.

58.11 The 'Access and Correction' principle, unlike the 'Data Quality' principle, refers to information being 'not misleading'.[13] It is sufficient that the 'not misleading' requirement only be contained in the 'Access and Correction' principle.[14] It is difficult for credit providers or credit reporting agencies to determine whether personal information is 'not misleading'—for example, because of surrounding circumstances of which they may not be aware—when collecting personal information or maintaining databases. When rights of correction are exercised, however, views may be formed more easily on whether credit reporting information, in a specific context, is or is not misleading.

58.12 The new *Privacy (Credit Reporting Information) Regulations* will prescribe the permissible content of credit reporting information. Information that is specifically permitted to be collected by the regulations can be assumed to be 'relevant' for the purposes of the recommended 'Data Quality' principle. Consequently, the relevance requirement will not place any additional obligations on credit providers or credit reporting agencies.

---

9 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

10 Veda Advantage, *Submission PR 498*, 20 December 2007.

11 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

12 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [54.71].

13 See Ch 29.

14 In Ch 59, the ALRC concludes that the correction provisions of s 18J of the *Privacy Act* need not be incorporated in the new regulations because this would largely duplicate provisions of the 'Access and Correction' principle.

58.13 The ALRC is of the view that general data quality obligations need not be incorporated in the new *Privacy (Credit Reporting Information) Regulations*. The ALRC's approach to reform of the credit reporting provisions is that the new regulations should be drafted to contain only those requirements that are different or more specific than those provided for in the model UPPs.[15] The data quality provision in the new regulations proposed in DP 72 would largely duplicate the provisions of the 'Data Quality' principle in the model UPPs[16] and is, therefore, unnecessary.

Data quality issues

58.14 Consumer groups and regulators have identified ongoing problems with the data quality of credit reporting information. Other stakeholders also provided perspectives on the extent and nature of data quality problems in the credit reporting system. This chapter highlights a number of specific issues concerning data quality before discussing means to ensure and improve data quality more generally.

58.15 Where specific concerns about data quality are serious and well-defined, and the solution is reasonably clear, it may be appropriate to deal with them through specific provisions of the new *Privacy (Credit Reporting Information) Regulations*. In other cases, matters may be dealt with more effectively through detailed data quality requirements in the credit reporting code,[17] subject to the overriding obligation to ensure that personal information is accurate, complete, up-to-date and relevant under the 'Data Quality' principle.

Statute-barred debts

58.16 The *Credit Reporting Code of Conduct* states that a credit provider must not give to a credit reporting agency information about an individual being overdue in making a payment where recovery of the debt by the credit provider is barred by the statute of limitations.[18] Section 18E(1)(ba)(i) of the *Privacy Act* prevents defaults from being listed against a guarantor's credit information file where a credit provider is 'prevented under any law of the Commonwealth, a State or a Territory from bringing proceedings against the individual to recover the amount of the overdue payment'.

58.17 There is, however, no parallel provision applying to the credit information files of other individuals. In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the

15 See Rec 54–2.
16 See Ch 27.
17 See Rec 54–9.
18 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [2.8]. See also *B v Credit Provider* [2004] PrivCmrA 2; *Q v Credit Provider 2* [2004] PrivCrimA 16.

Commonwealth, a State or a Territory from bringing proceedings against the individual to recover the amount of the overdue payment.[19]

Submissions and consultations

58.18 Stakeholders generally agreed that the new regulations should prohibit expressly the listing of statute-barred debts and ensure that borrowers and guarantors are treated consistently.[20]

58.19 The Australasian Retail Credit Association (ARCA) agreed with such a prohibition, but considered that the relevant provisions should be located in the credit reporting code, rather than in regulations.[21] ARCA and Veda Advantage emphasised that the implementation of the recommendation should not prevent the listing of defaults before bankruptcy.[22] ARCA stated:

> In the instance of bankruptcy, pre-existing listings should remain on the record with no requirement to delete all listings predating the bankruptcy. Those listings will remain for the usual retention period and the listing of the bankruptcy will inform the status of those debts.[23]

58.20 The Australian Finance Conference (AFC) noted that the law in relation to the collection of statute-barred debts is extremely complex, particularly because of the lack of uniformity between the legislative requirements in the different states and territories.[24]

ALRC's view

58.21 The rationales for statutory limitation periods on the enforceability of debts have been described as follows:

> First, as time goes by, relevant evidence is likely to be lost. Second, it is oppressive, even 'cruel', to a defendant to allow an action to be brought long after the circumstances which gave rise to it have passed. Third, people should be able to

---

19 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 54–1.

20 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Veda Advantage, *Submission PR 498,* 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Australian Finance Conference, *Submission PR 398,* 7 December 2007. The Mortgage and Finance Association of Australia opposed the proposal: Mortgage and Finance Association of Australia, *Submission PR 344,* 19 November 2007.

21 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007. Also: GE Money Australia, *Submission PR 537,* 21 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

22 Veda Advantage, *Submission PR 498,* 20 December 2007; Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007. On a bankruptcy, the bankrupt is discharged from all provable debts and creditors are prevented by law from taking action to recover those debts—although they may then lodge claims in bankruptcy with the trustee in bankruptcy: See *Bankruptcy Act 1966* (Cth).

23 Australasian Retail Credit Association, *Submission PR 352,* 29 November 2007. See *Bankruptcy Act 1966* (Cth).

24 Australian Finance Conference, *Submission PR 398,* 7 December 2007.

> arrange their affairs and utilise their resources on the basis that claims can no longer be made against them … The final rationale for limitation periods is that the public interest requires that disputes be settled as quickly as possible.[25]

58.22 While making an adverse credit listing is not the same as taking legal action to recover a debt, both actions may have negative consequences for the individual concerned and, with the passage of time, be more difficult to contest. Allowing the listing of statute-barred debts on credit information files is inconsistent with the public policy behind statutory limitation periods. The new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of statute-barred debts.

58.23 At law, proceedings to recover a statute-barred debt can be commenced in all jurisdictions except New South Wales. The legislation in other states provides a complete defence to legal proceedings, but does not extinguish the underlying debt.[26]

58.24 The new *Privacy (Credit Reporting Information) Regulations* should, therefore, prohibit the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a state or a territory from bringing proceedings against the individual to recover the amount of the overdue payment; or where any relevant statutory limitation period has expired.

Recommendation 58–1 The new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a state or a territory from bringing proceedings against the individual to recover the amount of the overdue payment; or where any relevant statutory limitation period has expired.

Schemes of arrangement

58.25 There is some ambiguity about the application of credit reporting provisions where the individual enters into a new arrangement with the credit provider to repay the debt, such as by entering into a scheme of arrangement.

58.26 Under the *Credit Reporting Code of Conduct*, a note indicating that a scheme of arrangement has been entered into by the individual and a credit provider only may be listed where an overdue payment or serious credit infringement previously has been listed.[27] OPC guidance states that

---

25 *Brisbane South Regional Health Authority v Taylor* (1996) 186 CLR 541, 552–553.

26 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

27 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [2.10].

> A credit provider may only report an arrangement for repayment to a credit reporting agency where the arrangement relates to an overdue payment or serious credit infringement which has been reported by the credit provider to the credit reporting agency. An arrangement for repayment may only be reported to a credit reporting agency where it is a formal written arrangement involving a substantial renegotiation of the terms of the loan. An arrangement would normally involve a significant variation of the individual's obligations with regard to one or more of the main elements of the contract such as the period of the loan, or the size and frequency of repayments. For [these purposes] an arrangement would not include, for example, a verbal agreement to allow a one-off late payment.[28]

58.27 In its credit reporting advice summaries, the OPC has stated that where a scheme of arrangement is entered into the 'new situation is not regarded as being information about the same default as the original entry'.[29] If payments become overdue under the new arrangement, therefore, a new default entry may be listed and remain on the individual's credit information file for a further five-year period.

Discussion Paper proposal

58.28 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should provide that, where the individual has entered into a new arrangement with a credit provider to repay an existing debt, such as by entering into a scheme of arrangement with the credit provider, an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information for the full five-year period permissible under the regulations.[30]

Submissions and consultations

58.29 Industry and consumer stakeholders generally supported the ALRC proposal.[31] The OPC submitted that the new regulations also should provide that an overdue payment under the new arrangement only may be listed after the requirements for listing a default have been met.[32] The OPC agreed that the definition of schemes of arrangement should be consistent with the current interpretation in the *Credit Reporting Code of Conduct*.[33]

58.30 ARCA noted that it has developed standards for reporting schemes of arrangement to credit reporting agencies. The purpose of the standards is to encourage ARCA members to use the reporting of schemes of arrangements 'more consistently as

---

28 Ibid, [55E].

29 Office of the Privacy Commissioner, *Credit Reporting Advice Summaries* (2001), [9.3].

30 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 54–2.

31 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Veda Advantage, *Submission PR 498,* 20 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007. The Australian Finance Conference stated that this matter should be dealt with in 'protocols' rather than by regulation: Australian Finance Conference, *Submission PR 398,* 7 December 2007.

32 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007

33 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [55E].

an indication that the creditor and the defaulter have reached a mutual agreement for the resolution of the outstanding debt'. The ARCA standard departs from existing practices by allowing a scheme of arrangement to be listed without the need for a default listing; and anticipates that the record of a scheme of arrangement will be deleted from credit reporting information after a period shorter than that applicable to default listings.[34]

ALRC's view

58.31 If an overdue payment under a scheme of arrangement recommences a new five-year listing period, an individual may be subject to adverse credit reporting information resulting from a default first made ten (or more) years ago. On the other hand, if a new listing period is not commenced, an individual's credit reporting information may not show that the individual is in default under a scheme of arrangement because the time period for the original debt has expired.

58.32 The preferable position is that a new listing period should commence. This is consistent with the OPC's interpretation of the existing provisions of Part IIIA. Any other position may lead to confusion about what constitutes the 'same' debt, including for example, where several debts are consolidated.

58.33 The *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt—such as by entering into a scheme of arrangement with the credit provider—an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information for the full five-year period permissible under the regulations.

58.34 For these purposes, a new credit arrangement should mean a formal written arrangement involving a substantial renegotiation of the terms of the loan. As stated in existing OPC guidance, an arrangement would normally involve a significant variation of the individual's obligations with regard to one or more of the main elements of the contract such as the period of the loan, or the amount and frequency of repayments.[35]

58.35 A related issue is whether regulation should permit a scheme of arrangement to be listed, without the need for a default to be listed first. It has been suggested that such a listing could be made subject to a shorter retention period than other adverse listings.

58.36 Arguably, such a reform would encourage credit providers to assist individual consumers to manage potential default and avoid the detrimental implications of a

---

34 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

35 See Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [55E]. This would include changes to a debtor's obligations under the *Consumer Credit Code* ss 66–67.

default listing. Any such proposal would need to 'balance the prevention of over-indebtedness with the desirability of preserving consumer options to reduce their financial difficulties by refinancing on more favourable terms'.[36]

58.37 Such a reform would require changes to recommended provisions with respect to the permitted content of credit reporting information;[37] and maximum permissible periods for retention of credit reporting information.[38] The ALRC is not convinced that allowing the reporting of schemes of arrangement without a default report being listed first is desirable—especially in the absence of any significant support from consumer groups for such a reform.

Recommendation 58–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt—such as by entering into a scheme of arrangement with the credit provider—an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information for the full five-year period permissible under the regulations.

Reporting overdue payments

58.38 Section 18E(1)(b)(vi) permits the inclusion in credit information files of information that is a record of:

> (vi) credit provided by a credit provider to an individual, being credit in respect of which:
>
> (A) the individual is at least 60 days overdue in making a payment, including a payment that is wholly or partly a payment of interest; and
>
> (B) the credit provider has taken steps to recover the whole or any part of the amount of credit (including any amounts of interest) outstanding …

58.39 Stakeholders raised a range of issues concerning the timing, calculation and multiple listing of overdue payments under this provision.

---

36 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 110, rec 26.

37 See Ch 56.

38 See Rec 58–5.

Timing

58.40 There is no maximum period of time before which an overdue payment must be listed[39] and the default reporting practices of credit providers vary considerably.[40] For example, there can be a significant delay (of three years or more in some cases) between a payment falling due and a telecommunications provider reporting the default to a credit reporting agency.[41]

Calculation

58.41 Section 18E(1)(b)(vi) does not deal expressly with reporting the amount of debt, and there is some uncertainty about the amount of debt that should be reported in respect to particular defaults. The position is complicated by the fact that some credit contracts have acceleration clauses. An acceleration clause is a term of a contract providing that on the occurrence or non-occurrence of a particular event (such as an overdue payment), the credit provider becomes entitled to immediate payment of all, or a part of, an amount under the contract that would not otherwise have been immediately payable.[42]

58.42 In the OPC's view, under s 18E(1)(b)(vi), 'the aggregate components of the listed amount must all be 60 days overdue'. The OPC suggested, nevertheless, that this provision may 'need to be re-drafted to make this position clearer'.[43] Some stakeholders considered that the rules should clarify that changes to amounts owing should be made by updating the original default—that is, by altering rather than adding information.[44]

Multiple listing

58.43 Other concerns relate to multiple adverse listings in respect of the same debt. Multiple listing may occur in a range of circumstances, including:

- A credit provider lists an overdue payment and then makes further listings to update the amount, or record another overdue payment for the same debt. This can extend the period that an overdue payment listing remains on a credit information file—potentially to the maximum term of the loan plus the five-year period prescribed by s 18F(2)(c).

---

39 Subject to *Privacy Act 1988* (Cth) s 18E(1)(ba) (dealing with statute-barred debts and guarantors); s 18F (deletion of information from credit information files).

40 See also the discussion of reciprocity and compulsory reporting in Ch 55.

41 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

42 *Consumer Credit Code* s 84.

43 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

44 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 28.

- A credit provider assigns a debt and the assignee automatically lists the overdue payments without checking whether the credit provider has already listed the debt; or because the assignee uses information different from that used by the original credit provider—making it difficult to determine whether the debt is the same debt.

- A credit provider lists an overdue payment and later lists a serious credit infringement with respect to the same debt. This can extend the period that an adverse listing remains on a credit information file—potentially to five years plus the seven year period prescribed by s 18F(2)(g).

58.44 Stakeholders confirmed a continuing problem with multiple listings.[45] The Telecommunications Industry Ombudsman noted, for example, that it is not uncommon for consumers to have multiple contacts with a telecommunications service provider in order to make repayment arrangements. This can sometimes lead to multiple default listings, extending the period of adverse listing for the same debt.[46]

58.45 The credit reporting provisions do not clearly prohibit multiple listing. The OPC takes the view—based on the interaction between ss 18E and 18F—that multiple listings for the same default are not permitted by Part IIIA.[47]

Linking files

58.46 A related issue concerns the linking of credit information files. Credit reporting information may be inaccurate because the individual has been identified incorrectly and credit reporting agencies may seek to avoid incorrect identification by linking files. For example, Veda Advantage stated that, where an individual 'uses two or more sets of identity details to obtain credit, we will hold a file for each identity and link them via a cross reference segment'.[48]

58.47 In practical terms, the linking of files means that when an affected individual makes a credit application and the credit provider makes an inquiry, all the linked files can be accessed.[49] It has been suggested that there should be provisions to regulate the linking of credit information files. The OPC has expressed concern that individuals may not be notified when their credit information file has been linked, and are unlikely to become aware of the linkage unless they are refused credit.[50]

---

45 Legal Aid Queensland, *Submission PR 292*, 11 May 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Min-it Software, *Submission PR 236*, 13 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007.

46 Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007.

47 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

48 Veda Advantage, *Submission PR 272*, 29 March 2007.

49 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

50 Ibid.

Discussion Paper proposal

58.48 In DP 72, the ALRC expressed the view that detailed data quality requirements should generally be dealt with in the credit reporting code. For example, the means to ensure consistency in the timing and calculation of reporting overdue payments and to avoid multiple listings were considered to be matters that should be pursued through a credit reporting code, rather than in regulations.[51]

58.49 The ALRC proposed that the credit reporting code should promote data quality by mandating procedures to ensure consistency and accuracy in the reporting of overdue payments and other personal information by credit providers. These procedures should deal with matters including:

- the timeliness of the reporting of personal information, such as overdue payments;
- the calculation of overdue payments for credit reporting purposes;
- obligations to prevent the multiple listing of the same debt;
- the updating of personal information reported, including where schemes of arrangement have been entered into; and
- the linking of credit reporting information where it is unclear whether the information relates to more than one individual with similar identifying details or to one individual who has used different identifying details.[52]

Submissions and consultations

58.50 There is consensus between industry and consumer groups about the importance of ensuring quality of credit reporting information. As stated by Abacus–Australian Mutuals, ensuring data quality is 'one of the biggest challenges for all users—consumers and business alike—of the credit reporting systems'.[53] The Consumer Credit Legal Centre (NSW) (CCLC) noted:

> Inaccuracies disadvantage consumers because they create the potential to be unfairly denied credit and pursued for debts that do not belong to them. It also disadvantages credit providers because they are less able to rely on credit report information as an accurate gauge of a person's creditworthiness and leads to inefficiencies in the credit system.[54]

---

51 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [54.17], [54.26].
52 Ibid, Proposal 54–5.
53 Abacus–Australian Mutuals, *Submission PR 278*, 10 April 2007.
54 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 123.

58.51 There is less agreement about the extent of existing data quality problems, or what should be done to remedy them. Submissions from consumers and industry highlighted a range of problems with the accuracy, timeliness and completeness of credit reporting information. On the other hand, some degree of data inaccuracy may be expected in a high-volume and complex information-processing environment such as credit reporting. Veda Advantage submitted:

> Despite the anecdotal evidence to the contrary, independent research demonstrates that the data quality is very high given the highly transactional nature of the data base with over 80,000 real time transactions a day.[55]

Role of the credit reporting code

58.52 There was broad agreement that the credit reporting code should deal with operational data quality issues.[56] Some stakeholders submitted, however, that a number of the data quality issues listed in the ALRC's proposal should be covered by the new regulations.[57]

58.53 The Cyberspace Law and Policy Centre, for example, stated that it supported 'an industry code to deal with residual data quality issues' but, as discussed below, the timeliness of overdue payment listing and multiple listing should be dealt with in the regulations.

> We disagree with the ALRC that most data quality requirements can be left to an industry code … Experience to date shows that there are a range of known data quality problems in credit reporting which the existing regulatory framework has been unable to resolve. While there has been significant progress on some of these issues through voluntary industry–consumer consultations, we submit that more of the known issues need to be addressed in the Regulations.[58]

---

55 Veda stated that a 2006 pilot study of 400 consumers who had recently obtained a copy of their credit information file showed: 95% of the credit file segments were entirely accurate; 4% contained a minor error, such as incorrect spelling of personal details; and 1% reported a major error with their file, such as an incorrect credit inquiry or default report listing: Veda Advantage, *Submission PR 272*, 29 March 2007.

56 GE Money Australia, *Submission PR 537*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. Telstra objected to locating data quality provisions in the proposed code, on the basis that it would lead to 'inflexibility and inappropriate results': Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

57 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

58 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. Also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

58.54 Similarly, the OPC agreed that 'detailed operational' matters should be dealt with in the proposed credit reporting code, but considered that a range of matters relating to data quality should be prescribed in the new regulations.[59]

58.55 Galexia criticised the proposed allocation of data quality obligations between the legislation and the credit reporting code.

> The ALRC appears to be suggesting an unusual regulatory arrangement—where the issue is simple and the solution is clear the requirements can be set out in the Regulations, but where the issue is complex and the solution is unclear it should be dealt with by a potential industry Code.[60]

58.56 Galexia stated that the better approach would be for 'core data accuracy' requirements to be located in the new regulations, with supplementary industry rules about data consistency addressed in the code.[61]

Reporting overdue payments

58.57 Stakeholders emphasised the need for more consistency in relation to the reporting of overdue payments.[62] Some disagreed, however, that these data quality requirements should be dealt with in the credit reporting code rather than in regulations.

58.58 The OPC stated that credit reporting requires a certain level of prescription, including in relation to data quality obligations. The OPC submitted that matters relating to data quality that should be prescribed in the new regulations include:

- a maximum period of time by which listing of an overdue payment must occur;
- a general principle for the calculation of overdue payments, based on the existing requirement in s 18E(1)(b)(vi);
- a prohibition on multiple listings in relation to the same overdue payment, but allowing credit providers to update listings; and
- a general requirement for credit providers and credit reporting agencies to take reasonable steps to prevent inaccuracies arising from the linking of credit files.[63]

---

59 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
60 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.
61 Ibid.
62 For example, Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.
63 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

58.59 Other stakeholders suggested that regulations should provide for a maximum period of time—such as 12 months[64]—before which an overdue payment must be listed.[65] Legal Aid Queensland stated:

> This would prevent credit providers listing many years after the default, prevent listing after the limitation period has expired and prevent arguments by the credit provider that the consumer has revived the debt and they are therefore entitled to list.[66]

58.60 The Cyberspace Law and Policy Centre also submitted that the new regulations should provide that overdue payments must be listed within 12 months; and should allow the updating of an existing listing to avoid multiple listing of the same default.[67] The Financial Counsellors Association of Queensland submitted that the regulations should require credit providers to provide updating information to a credit reporting agency within 30 days; and credit reporting agencies to process the update within 14 days of receipt.[68]

Systemic data quality issues

58.61 Several stakeholders submitted that the new regulations or the credit reporting code should also place obligations on credit providers and credit reporting agencies to deal with systemic data quality issues.[69]

58.62 The Consumer Action Law Centre submitted that the code should be expanded to impose an obligation on credit providers and credit reporting agencies to report systemic errors to the OPC.

> Reporting could include information about the credit provider's (or CRA's) response to the errors, and subsequent reporting of the action taken. Failure to report systemic issues should lead to significant penalties, as we suspect that otherwise there would be little incentive to make such reports. Similar obligations to report significant breaches of regulatory obligations to the regulator in the financial services sector has contributed to many systemic issues being identified and addressed by industry in a timely manner.[70]

---

64 Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 12.

65 Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 12; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

66 Legal Aid Queensland, *Submission PR 489,* 19 December 2007.

67 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

68 Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007.

69 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Consumer Action Law Centre, *Submission PR 510,* 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

70 Consumer Action Law Centre, *Submission PR 510,* 21 December 2007.

58.63 The Cyberspace Law and Policy Centre supported this suggestion and submitted that the new regulations (rather than the code) should 'require credit providers and credit reporting agencies to report systemic data quality problems, and the remedial action taken, to the Privacy Commissioner'.[71] The Centre submitted that the regulations should contain obligations similar to those in the existing *Credit Reporting Code of Conduct*, which provide that a credit reporting agency, when it becomes aware that information supplied by a credit provider may be inaccurate, should request the credit provider to investigate the accuracy of other files that may be similarly affected.[72]

ALRC's view

Prescribing data quality standards

58.64 Determining whether particular credit reporting information is 'accurate, up-to-date' and 'complete' in terms of the 'Data Quality' principle—and 'not misleading' in terms of the access and correction provision of the new regulations[73]—will not always be a simple matter. For example, where a debt is disputed, the 'accuracy' of the information may be dependent on a determination of the legal rights of the parties. Information may be 'accurate' in terms of reflecting, for example, the amount owed by an individual at the time a credit report is issued, but not comply with data quality standards because the individual is not 60 days overdue, as required by the legislation.[74]

58.65 The concept of completeness is also problematic, for example, in relation to the timing of default reporting. There is a tension, in this context, between the use of credit reporting in credit risk assessment and debt management (and debt collection). At the risk assessment 'front-end', the concern of credit providers is that the credit report provides up-to-date and complete information relevant to the credit worthiness of the individual to whom it relates. Once an individual has gone into arrears, however, a credit provider's decision on whether to list the default may be subject to other considerations—including how best to encourage repayment or to manage over commitment (for example, through a scheme of arrangement).

58.66 Privacy principles should ensure that credit reporting agencies and credit providers are obliged to take reasonable steps to ensure the data quality of credit reporting information. The complexity of data quality issues in credit reporting means that more prescriptive regulation is generally undesirable. Prescriptive requirements may unnecessarily increase the cost of compliance with the *Privacy Act* and transaction costs in the finance industry generally, without any significant benefit in terms of data quality.

---

71 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
72 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [1.4].
73 See Ch 59.
74 *Privacy Act 1988* (Cth) s 18(1)(vi)(A).

Overdue payment reporting

58.67 In particular, consistency in the timing and calculation of default reporting is a matter that should be pursued through the credit reporting code. In this context, credit providers, through ARCA, have been working towards the development and implementation of industry reporting standards dealing with the reporting of overdue payments; and schemes of arrangement.[75]

58.68 When developing the default reporting standard, ARCA examined ways to reconcile differences between credit providers' internal accounting and reporting procedures and the reporting of overdue payments allowed by the credit reporting provisions of the *Privacy Act*. ARCA's aim is to encourage credit providers to move to a consistent default reporting standard, based on reporting the full amount outstanding at the time of listing.[76]

58.69 Instead of improving data quality, attempts to prescribe approaches to these matters by regulation would create new difficulties and ambiguities. It also could constrain the ability of industry to respond flexibly to data quality and consistency problems. In particular, a separate legislative prohibition on multiple listing is unnecessary, given that multiple listing of the same debt probably would constitute a breach of the requirements in the UPPs that credit reporting information be 'accurate' and 'not misleading'.

Conclusion

58.70 With some exceptions (as in the case of the listing of statute-barred debts), it is more appropriate to leave detailed data quality requirements to be dealt with in the recommended credit reporting code. This code should be developed with input from consumer groups and regulators.

58.71 If industry self-regulation is not successful in addressing the existing problems, including through a credit reporting code, further regulation should be considered—at least with respect to some basic elements of default reporting, such as time limits and requirements to report the full amount outstanding at the time of listing.

58.72 In Chapter 54, the ALRC recommends that the Australian Government, five years from the commencement of the new *Privacy (Credit Reporting Information) Regulations* should initiate a review of the regulations.[77] One matter this review should consider is whether further regulation is required to ensure the data quality of credit reporting information. If the review indicates that industry self-regulation is not

---

75 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007, App 6 'ARCA standard on default reporting as agreed with BFSO October 2006; App 7 'ARCA standard on recording schemes of arrangement'.

76 Ibid.

77 Rec 54–8.

successful in addressing data quality problems such as those discussed in this chapter, further regulation should be considered.

Recommendation 58–3 The credit reporting code should promote data quality by setting out procedures to ensure consistency and accuracy of credit reporting information. These procedures should deal with matters including:

(a) the timeliness of the reporting of credit reporting information;

(b) the calculation of overdue payments for credit reporting purposes;

(c) obligations to prevent the multiple listing of the same debt;

(d) the updating of credit reporting information; and

(e) the linking of credit reporting information relating to individuals who may or may not be the same individual.

Data quality obligations of credit reporting agencies

58.73 Much of the credit reporting information provided by credit reporting agencies to their subscribers is supplied to agencies by credit providers. Credit reporting can be described, to some extent, as operating on an 'honour system'—in that credit reporting agencies do not have the capacity readily to check the accuracy of the information given to them by credit providers.

58.74 While the 'Data Quality' principle in the model UPPs requires credit reporting agencies to 'take reasonable steps' to ensure the accuracy of information, it has been suggested that, given the high volume of information handled by credit reporting agencies, more detailed obligations are required.[78]

58.75 The New Zealand *Credit Reporting Privacy Code 2004* (the NZ Code) provides one model for the imposition of obligations that could be placed on credit reporting agencies to ensure the data quality of credit reporting information, including that supplied to them by credit providers.[79] Under the NZ Code agencies must:

78 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.11].

79 The NZ Code requires credit reporting agencies to enter into subscriber agreements that comply with the provisions of a schedule to the Code: *Credit Reporting Privacy Code 2004* (NZ), r 8(3)(a), sch 3.

> (b) establish and maintain controls to ensure that, as far as reasonably practicable, only information that is accurate, up to date, complete, relevant, and not misleading is used or disclosed;
>
> (c) monitor information quality and conduct regular checks on compliance with the agreements and controls;
>
> (d) identify and investigate possible breaches of the agreements and controls;
>
> (e) take prompt and effective action in respect of any breaches that are identified; and
>
> (f) systematically review the effectiveness of the agreements and controls and promptly remedy any deficiencies.[80]

Discussion Paper proposal

58.76 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

- enter into agreements with credit providers that contain obligations to ensure data quality in the information credit providers provide to credit reporting agencies;
- establish and maintain controls to ensure that only information that is accurate, complete, up-to-date and relevant is used or disclosed;
- monitor data quality and audit compliance with the agreements and controls; and
- identify and investigate possible breaches of the agreements and controls.[81]

Submissions and consultations

58.77 The OPC supported the ALRC's proposal.[82] The OPC also suggested that it produce guidance for credit providers and credit reporting agencies about what constitutes 'reasonable steps' to promote and maintain the accuracy of credit reporting information.[83]

58.78 Industry and consumer stakeholders provided considerable, if qualified, support for the ALRC's proposal.[84] ARCA supported the imposition of new data quality

---

80 Ibid, r 8(3).

81 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 54–3.

82 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

83 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

84 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

obligations on credit reporting agencies, but submitted that these should be detailed in a code of conduct and not in the regulations.[85] GE Money agreed with the ARCA position, but noted that

> reliance on the credit reporting agencies alone to oversee data accuracy and management is problematic. Their willingness to 'enforce' may be compromised by the economics of the relationships—a reluctance to 'bite the hand that feeds'. Only independent oversight and enforcement will be workable.[86]

58.79 The Consumer Action Law Centre supported the ALRC's proposal but noted that the key to the effectiveness of these provisions will be how the regulations are enforced. The Centre stated:

> As well as having an obligation to enter into particular agreements with credit providers, credit reporting agencies should have an obligation to enforce compliance with those agreements.[87]

58.80 Veda Advantage stated that the ALRC's proposal should include a requirement that credit providers and credit reporting agencies must agree to appropriate deadlines for supplying information when an agency is undertaking an investigation related to data quality.

58.81 Some stakeholders opposed the imposition of new data quality obligations on credit reporting agencies. The AFC questioned why specific provisions are required that 'effectively restate' the obligations under the 'Data Quality' principle.[88] Telstra objected to the proposal, on the basis that was 'an unnecessary, over-prescriptive approach, inconsistent with outcomes-based regulatory principles'.[89]

ALRC's view

58.82 Consumer groups have expressed concerns that there are no adequate incentives for credit reporting agencies or credit providers to correct systemic flaws in the credit reporting system, in part because the cost of dealing with a small number of complaints is less than the cost of ensuring the data is accurate in the first place.[90]

---

85 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. Dun and Bradstreet submitted that such obligations be included in 'contractual terms' as well as in the code of conduct: Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007.

86 GE Money Australia, *Submission PR 537*, 21 December 2007.

87 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007. The Centre also referred, in this context, to the importance of auditing (discussed below).

88 Australian Finance Conference, *Submission PR 398*, 7 December 2007. EnergyAustralia stated that it 'is hard to see how further regulation could ensure greater accuracy on the part of credit providers' EnergyAustralia, *Submission PR 229*, 9 March 2007.

89 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

90 See, eg, Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 135.

58.83 Credit reporting agencies should take more responsibility for ensuring data quality. This imperative is recognised by agencies themselves. Veda Advantage stated, for example, that a statutory obligation on the credit reporting agencies to be satisfied that credit providers are able to comply with data quality obligations would 'help [to] ensure regulatory objectives are met'.[91]

58.84 The ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* impose obligations on credit reporting agencies to monitor the data quality of information provided to them by credit providers, including through audit, discussed below. A provision containing similar obligations to those contained in the NZ Code should be included in the new *Privacy (Credit Reporting Information) Regulations*, to encourage the development of audit and other processes to ensure data quality.

58.85 The new *Privacy (Credit Reporting Information) Regulations* should also provide that credit reporting agencies must enter into agreements with credit providers that contain obligations to ensure the security of credit reporting information. Data security is discussed later in this chapter.

Recommendation 58–4 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

(a) enter into agreements with credit providers that contain obligations to ensure the quality and security of credit reporting information;

(b) establish and maintain controls to ensure that only credit reporting information that is accurate, complete and up-to-date is used or disclosed;

(c) monitor data quality and audit compliance with the agreements and controls; and

(d) identify and investigate possible breaches of the agreements and controls.

Auditing credit reporting information

58.86 The audit of credit reporting information may assist to ensure data quality. Under s 28A(1)(g) of the *Privacy Act*, the Privacy Commissioner has the function of auditing credit information files and credit reports held by credit reporting agencies and credit providers.

91 Veda Advantage, *Submission PR 272*, 29 March 2007.

58.87 The OPC review of the private sector provisions of the *Privacy Act* noted that the priority given by the OPC to its complaint-handling functions has diverted resources from other areas of responsibility, including auditing.[92] No credit reporting audits have been conducted since 2003–04.[93]

Submissions and consultations

58.88 In DP 72, the ALRC noted strong support for the use of the Privacy Commissioner's powers to audit credit reporting information.[94] For example, the Consumer Action Law Centre advocated that the Australian Government allocate more resources to the OPC to perform its auditing functions.

> In the credit reporting regulatory scheme, the OPC is both the complaints handler and the regulator. It is therefore even more important that it identify systemic issues or incidents of non-compliance with the scheme and take action where appropriate. Undertaking audits is the key way in which information about non-compliance may be obtained proactively, with complaints received the key way in which such information is obtained reactively.[95]

58.89 The OPC submitted that the audit power under s 28A(1)(g) should be retained in the new *Privacy (Credit Reporting Information) Regulations*. Other stakeholders noted the practical barriers to audits by the OPC, given the scale of the credit reporting system, and the complexity of agreements and operating systems.[96] One suggested solution is for third parties to carry out privacy audits on behalf of the OPC.[97]

58.90 Another possibility, suggested by a number of stakeholders, is to place more formal obligations on credit reporting agencies to ensure the data quality of information provided by their subscribers, including through audit processes.[98] The Australian Privacy Foundation submitted that credit reporting agencies should be

---

92 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 160. While the OPC Review referred to auditing of Commonwealth government agencies specifically, diversion of resources may also have affected credit reporting audits.

93 See Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [4.20]–[4.21].

94 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007) rec 55. See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [54.44]–[54.55].

95 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

96 Experian Asia Pacific, *Submission PR 228*, 9 March 2007; Confidential, *Submission PR 227*, 9 March 2007.

97 The costs of the audit would be borne by the credit providers themselves: Confidential, *Submission PR 227*, 9 March 2007.

98 Legal Aid Queensland, *Submission PR 292*, 11 May 2007; Queensland Law Society, *Submission PR 286*, 20 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Veda Advantage, *Submission PR 272*, 29 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 41.

required to include data quality obligations in subscriber agreements; monitor and conduct regular checks on quality; and investigate any possible breaches.[99] The Consumer Action Law Centre stated:

> Some auditing (internal and/or external) by credit reporting agencies, and a requirement to report to the regulator could be an efficient way of monitoring some aspects of compliance by the credit provider, as well as the credit reporting agency.[100]

58.91 Other stakeholders highlighted the possible role of self-auditing by credit providers.[101] The OPC, for example, supported the 'promotion and implementation of self auditing systems for credit reporting compliance within the credit reporting industry', and recommended that the credit reporting code include procedures for the self-auditing of credit reporting information.[102]

ALRC's view

58.92 In Chapter 47, the ALRC discusses the consolidation of the Privacy Commissioner's audit functions under the *Privacy Act*. The ALRC recommends that the Act be amended to empower the Privacy Commissioner to conduct 'Privacy Performance Assessments' of personal information maintained by an organisation for the purpose of ascertaining whether the records are maintained according to the model UPPs, privacy regulations, rules or any privacy code that binds the organisation.[103] If this recommendation is implemented, it would be unnecessary to retain s 28A(1)(g).

58.93 Auditing is an important mechanism by which to ensure data quality and security. It is an important tool that the OPC should be able to use for a range of compliance purposes, including in credit reporting contexts. In practice, an OPC audit of credit reporting information must be used selectively, as it is complex and resource intensive.

58.94 The ALRC does not recommend the implementation of any general requirement on agencies or organisations to self-audit. Such a requirement would place a demand on the OPC's resources in monitoring the self-audit process, and a compliance burden on agencies and organisations.[104]

58.95 The audit of credit reporting information by a credit reporting agency or credit provider may be required, in some circumstances, to comply with the obligation to 'take reasonable steps' under the 'Data Quality' or 'Data Security' principles. In addition, the ALRC recommends that the new *Privacy (Credit Reporting Information)*

---

99 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.

100 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

101 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 292*, 11 May 2007; Queensland Law Society, *Submission PR 286*, 20 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Veda Advantage, *Submission PR 272*, 29 March 2007.

102 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

103 Rec 47–6.

104 See Ch 47.

Regulations impose obligations on credit reporting agencies to ensure the quality of credit reporting information.[105] These include an obligation on agencies to audit compliance by credit providers with agreements and monitor controls relating to data quality.

58.96 Finally, as discussed above, the ALRC recommends that the credit reporting code promote data quality by setting out procedures to ensure consistency and accuracy of credit reporting information. These procedures could include the self-auditing of credit reporting information. There would be no benefit in prescribing by regulation more specific audit obligations.

Data security

58.97 The 'Data Security' principle in the model UPPs provides that an agency or organisation must take reasonable steps to:

- protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure; and

- destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.

58.98 In Part IIIA, credit providers and credit reporting agencies have an obligation under s 18G(b) to ensure that credit information files or credit reports are 'protected, by such security safeguards as are reasonable in the circumstances, against loss, against unauthorised access, use, modification or disclosure, and against other misuse'. Section 18G(c) provides that credit providers and credit reporting agencies must also, if it is necessary for credit reporting information to be given to a person 'in connection with the provision of a service to the credit reporting agency or credit provider', ensure that 'everything reasonably within the power of the credit reporting agency or credit provider is done to prevent unauthorised use or disclosure'.

58.99 In addition, Part IIIA contains provisions requiring credit reporting agencies to ensure that credit reporting information is deleted after the expiry of maximum permissible retention periods set out in s 18F. The deletion of credit reporting information is considered separately below.

58.100 A range of concerns about the security of credit reporting information has been identified by the OPC in the conduct of its credit reporting auditing functions. The security issues included: insufficient security of the manner in which passwords

105 Rec 58–4.

and user codes were provided to new subscribers; passwords of former employees not being automatically deactivated; and the poor security of passwords in the online environment, such as the storage of passwords by web browsers.[106] In addition, it was found that some credit providers did not have provisions in their service provider contracts regarding the security and confidentiality of information, even though these contractors can obtain access to personal information held by credit providers.[107]

58.101 In this Inquiry, the ALRC asked about issues raised by regulation dealing with the security of credit information files and credit reports and how these provisions operate in practice.[108] The ALRC received relatively little comment on data security issues in the context of credit reporting specifically.

Discussion Paper proposal

58.102 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* contain no equivalent to s 18G(b) and (c), dealing with the security of credit reporting information, as these obligations were adequately covered by the 'Data Security' principle.[109]

Submissions and consultations

58.103 Industry and consumer stakeholders agreed that the new regulations should contain no equivalent to s 18G(b) and (c) of the *Privacy Act*.[110]

58.104 Veda Advantage stated that it would not be necessary for the new *Privacy (Credit Reporting Information) Regulations* to modify the 'Data Security' principle. Veda submitted, however, that agreements between credit reporting agencies and credit providers should be required to cover data security, as well as data quality, obligations.

> With the potential increase in personal information shared under reform proposals, a significant potential harm arises from data breach. Accordingly the law should require that agreements cover this risk.[111]

---

106 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 65–66; Australian Government Attorney-General's Department, *Response to Questions on Notice for Attorney-General's Portfolio: Senate Legal and Constitutional Legislation Committee Additional Estimates 2003–2004, Questions 38 to 50*, undated, Answer to Q 42.

107 Australian Government Attorney-General's Department, *Response to Questions on Notice for Attorney-General's Portfolio: Senate Legal and Constitutional Legislation Committee Additional Estimates 2003–2004, Questions 38 to 50*, undated, Answer to Q 42.

108 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–6.

109 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 54–9.

110 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Australian Finance Conference, *Submission PR 294*, 18 May 2007.

111 Veda Advantage, *Submission PR 498*, 20 December 2007.

ALRC's view

58.105 The data security obligation in s 18G(b) provides an additional requirement, as compared to the 'Data Security' principle in the model UPPs, that personal information be protected from 'unauthorised use'. The 'Data Security' principle does, however, refer to the 'misuse' of personal information, which seems broad enough to cover unauthorised use. The data security obligation in s 18G(c) is not required because credit reporting information in the hands of an organisation other than a credit provider or credit reporting agency will be protected adequately by the UPPs.

58.106 The recommended 'Data Security' principle adequately covers credit reporting information and no separate provision dealing with data security is needed in the new *Privacy (Credit Reporting Information) Regulations*. The ALRC recommends, however, that the regulations provide that credit reporting agencies must enter into agreements with credit providers that contain obligations to ensure the security, as well as the quality, of credit reporting information. This recommendation is incorporated into Recommendation 58–4 above.

Deletion of credit reporting information

58.107 The 'Data Security' principle provides that an agency or organisation must take reasonable steps to 'destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law'.

58.108 Part IIIA, in contrast, contains detailed provisions requiring credit reporting agencies to ensure that personal information contained in credit information files is deleted after the expiry of maximum permissible retention periods set out in s 18F.[112] For example:

- information about overdue payments must be deleted five years after the day on which the credit reporting agency was informed of the overdue payment concerned;[113]
- information that, in a credit provider's opinion, an individual has committed a specific serious credit infringement must be deleted seven years after the information was included in the credit information file;[114] and
- a record of a bankruptcy order must be deleted seven years after the order was made.[115]

---

112 These periods are summarised in Ch 53.
113 *Privacy Act 1988* (Cth) s 18F(2)(c).
114 Ibid s 18F(2)(g). The definition of 'serious credit infringement' is discussed in Ch 56.
115 Ibid s 18F(2)(f).

Discussion Paper proposals

58.109 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide for the deletion by credit reporting agencies of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.[116]

58.110 The ALRC also proposed that the regulations provide for the deletion of information about voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.[117] The need for this proposal arose as a consequence of the ALRC's proposal to permit the collection of credit reporting information about all the types of personal insolvency administration available under the *Bankruptcy Act 1966* (Cth).[118]

Submissions and consultations

58.111 Stakeholders generally agreed that the new regulations should provide for the deletion of information as currently set out in s 18F.[119] Some stakeholders considered, however, that the specific retention periods should be located in the code of conduct, rather than in the regulations.[120]

58.112 Other stakeholders expressed the view that the maximum permissible retention periods currently applicable should be reviewed more closely.[121] The Cyberspace Law and Policy Centre submitted that the periods set out in s 18F need to be reviewed. In particular, the regulations should require the time period within which a default listing must be deleted 'to commence from the event rather than from the time of listing'.[122]

58.113 The OPC agreed that the maximum permissible retention periods should be based on those in s 18F, but suggested further consideration of whether

> time limits for adverse listings should be on the basis of set monetary amounts on a graduated scale, with the maximum permissible retention periods based on those

---

116 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 54–7.

117 Ibid, Proposal 54–8.

118 Ibid, Proposal 52–4.

119 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

120 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

121 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

122 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. As suggested by MasterCard Worldwide: MasterCard Worldwide, *Submission PR 237*, 13 March 2007.

> currently set out in s 18F of the Privacy Act applying to credit reporting information that relates to higher monetary amounts and shorter retention periods applying to lower monetary amounts.[123]

58.114 Others also favoured a 'more graduated' set of retention periods,[124] including a two year maximum permissible period for the retention of default listings for non-credit services such as telecommunications.[125]

58.115 The AFC suggested that the maximum permissible retention periods should take into account record-keeping obligations under other regulation such the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).[126] ING Bank was concerned about the impact of the periods prescribed by s 18F on identity verification. Section 18F, it was said,

> will potentially exclude customers, who do not represent a money laundering/terrorist financing risk, from being electronically verified if they have not applied for credit in some years.[127]

58.116 Veda Advantage submitted that credit reporting agencies should be able to 'continue to hold credit reporting information for the building of statistical models' beyond the retention periods prescribed by the regulations.[128] Veda advised that this is currently done by removing the information from an individual's 'credit information file', as that term is defined in the Act.[129]

58.117 Stakeholders provided support for the proposed five year maximum permissible retention period for information about voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act*.[130]

---

123 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007. The OPC earlier suggested that the listing period for defaults be reduced from five and seven years to periods of two and four years, respectively, for minor monetary amounts. The OPC also submitted that the ALRC consider shorter credit listing timeframes for minors: Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

124 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

125 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 15.

126 Australian Finance Conference, *Submission PR 398,* 7 December 2007.

127 ING Bank, *Submission PR 230,* 9 March 2007. See Ch 57 on the use of credit reporting information in electronic identity verification.

128 Veda Advantage, *Submission PR 498,* 20 December 2007.

129 *Privacy Act 1988* (Cth) s 6(1).

130 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Legal Aid Queensland, *Submission PR 489,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401,* 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371,* 30 November 2007.

58.118 The CCLC expressed concern about the listing of debt agreements under Part IX of the *Bankruptcy Act* and submitted that such listings, if permitted, should be removed when the debtor has satisfied their obligations under the agreement.[131] Conversely, some industry stakeholders disagreed with the proposal on the basis that the maximum permissible period of retention should be seven years, as is the case for information about bankruptcy orders.[132]

58.119 The OPC also submitted that the new regulations should specify how the data destruction obligations of the 'Data Security' principle apply in relation to credit reporting information. As noted above, the 'Data Security' principle requires agencies and organisations to 'destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law'. The OPC submitted that the application of this principle to credit reporting information would need to reflect that:

- The relevant purpose is that permitted by the UPPs as modified by the new *Privacy (Credit Reporting Information) Regulations*. For example, notwithstanding that information is needed for a purpose permitted by the UPPs, this should not circumvent the requirements to delete the credit reporting information under an equivalent to s 18F.

- Credit reporting information should be deleted at the expiry of the relevant maximum retention period, as currently provided under s 18F. To avoid any uncertainty, the option in the 'Data Security' principle to render the information 'non-identifiable' should not be applicable to credit reporting information.[133]

ALRC's view

58.120 The retention periods prescribed by s 18F provide an important protection for consumers. The consequences of an adverse listing can be serious. It is important that, after some reasonable period of time, the information should be considered spent, allowing the individual to 'repair' their credit record.

58.121 It would not be appropriate, in this context, to rely on the general provisions of the 'Data Security' principle, as this would leave credit reporting agencies with too much discretion. One stakeholder noted that the regulation of retention periods is 'an area in which more rather than less prescription is desirable'.[134]

---

131 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 34.

132 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

133 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

134 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007. Also Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.

58.122 There is some concern about the relationship between the maximum permissible periods for the retention of credit reporting information and other records under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth). The *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules) requires reporting entities to retain for seven years records of the provision of a designated service and related documents.[135]

58.123 The AML/CTF Rules state that these record-keeping requirements do not override Part IIIA of the *Privacy Act*.[136] The explanatory memorandum stated that this means that records retained in compliance with the AML/CTF Rules for longer than the maximum period permitted by the *Privacy Act* should only be used for purposes associated with fulfilling the requirements of the AML/CTF Rules. Credit reporting agencies and credit providers may, it said, retain credit reporting information that is covered by the record-keeping requirements of the AML/CTF Rules, as long as that information only is used for AML/CTF purposes.[137]

58.124 In any case, the use of credit reporting information for electronic identity verification, which the ALRC recommends be authorised expressly under the AML/CTF Act,[138] depends primarily on the availability of name, date of birth and address information. This information is not subject to a maximum permissible period of retention under s 18F.

58.125 The ALRC does not consider that there is any compelling case for change to the existing retention periods. Credit reporting information technology systems are built around these retention periods and changes may involve significant transition costs. The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F.

58.126 One exception involves personal insolvency information. As discussed in Chapter 56, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* permit credit reporting information to include all the types of personal insolvency information recorded on the National Personal Insolvency Index administered under the *Bankruptcy Regulations 1966* (Cth).[139] These include voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act*.

---

135 *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1) 2007* (Cth) pt 10.

136 Ibid r 105.

137 Replacement Explanatory Memorandum, Anti-money Laundering and Counter-Terrorism Financing Bill 2006 (Cth).

138 Rec 57–4.

139 Rec 56–4 and 56–5.

58.127 The ALRC considers that information about voluntary arrangements with creditors under Part IX and Part X should be subject to a five year retention period, rather than the seven years applicable to bankruptcy.[140] An individual who has come to a voluntary arrangement with creditors should not be in a worse position than other individuals who have defaulted.

58.128 Finally, there is no need for the new regulations to specify how the 'Data Security' principle applies in relation to the deletion of credit reporting information. The new regulations are to provide that credit reporting information should be deleted after the expiry of the relevant maximum permissible retention period. This specific obligation modifies and overrides the provisions of the 'Data Security' principle where credit reporting information is concerned.

Recommendation 58–5 The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.

Recommendation 58–6 The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of information about voluntary arrangements with creditors under Parts IX and X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.

140 Such a reform was supported by the OPC: Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007.

59. Access and Correction, Complaint Handling and Penalties

Contents

Introduction

59.1 In this chapter, the ALRC discusses the existing provisions of Part IIIA of the *Privacy Act 1988* (Cth) dealing with an individual's rights of access to, and correction of, credit reporting information. Recommendations on how these matters should be dealt with under the model Unified Privacy Principles (UPPs)[1] and the new *Privacy (Credit Reporting Information) Regulations* are made.

59.2 The chapter also examines complaint handling in credit reporting disputes by the Office of the Privacy Commissioner (OPC) and other complaint-handling bodies and processes. Penalties for breach of the new regulations are also discussed.

Access and correction obligations

59.3 The 'Access and Correction' principle in the model UPPs provides that, subject to a range of exceptions:

> If an agency or organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information …

59.4 The 'Access and Correction' principle also provides that if an organisation charges for providing access to personal information, those charges must not be excessive and must not apply to lodging a request for access.

59.5 Part IIIA contains similar provisions relating to personal information in credit information files and credit reports. Section 18H provides that credit reporting agencies and credit providers must take reasonable steps to ensure that individuals can obtain access to such files and reports.

59.6 There are, however, significant differences between the rights of access in s 18H and the 'Access and Correction' principle. These include the absence of exceptions to the rights of access in s 18H and the fact that, while the principle (like National Privacy Principle (NPP) 6.4) provides that access charges 'must not be excessive', s 18H is silent on charging of fees for access.

59.7 In relation to obligations to correct personal information, the 'Access and Correction' principle provides that an organisation must take such steps, if any, as are reasonable to correct the information so that it is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant. The principle also provides that other entities to whom the personal information has already been disclosed be notified, if requested to do so by the individual, and provided such notification would be practicable in the circumstances.

---

1 See Part D.

59.8 Further, if an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant, the individual may ask for a correcting statement to be associated with the information.

59.9 Section 18J(1) contains similar provisions requiring credit reporting agencies and credit providers to take reasonable steps to correct credit information files or credit reports to ensure these are accurate, up-to-date, complete and not misleading. In addition, s 18J(2) contains specific provisions dealing with the inclusion of correcting statements, on the request of an individual.[2]

Access and correction in practice

59.10 All major Australian credit reporting agencies provide individuals with access to their own credit reports on request and free of charge.[3] In many cases, an individual requests access to his or her credit reporting information because he or she has been refused credit.

59.11 Veda Advantage responds annually to approximately 260,000 credit access requests.[4] Veda provides access free of charge by post within 10 working days; or for $27 within one working day by email, facsimile or mail.[5] Dun and Bradstreet provides access free of charge by post within 10 working days; or for $25 posted by express mail within one working day.[6] Tasmanian Collection Service provides access to credit information files free of charge 'where the request relates to an individual's refusal of credit, or is otherwise related to the management of the individual's credit arrangements' and, otherwise, for $13.[7]

59.12 Some credit reporting agencies actively encourage individuals to obtain access to their own credit information files. The Veda Advantage website notes the benefits in doing so to 'ensure your information is accurate and up to date to avoid unwanted surprises when you next apply for credit'.[8] Veda also offers a service, named 'My Veda Alert', that, for a fee, notifies an individual whenever someone obtains the individual's credit information file or there is an addition or change to the information

---

2 Where a credit reporting agency or credit provider does not amend personal information as requested, the individual concerned may request that the credit reporting agency or credit provider include a statement of the correction, deletion or addition sought: *Privacy Act 1988* (Cth) s 18J(2). Under s 18J(3), a credit reporting agency or credit provider may refer a statement considered to be of undue length in the circumstances to the Privacy Commissioner for a decision on alteration of the statement.

3 Ibid s 18H does not require that access be free of charge to the individual concerned.

4 Veda Advantage, *Submission PR 498*, 20 December 2007.

5 Veda Advantage, *Discover Your Credit History* (2005) <www.mycreditfile.com.au> at 5 May 2008.

6 Dun & Bradstreet, *Your Individual Credit File* (2006) <www.dnb.com.au> at 5 May 2008.

7 Tasmanian Collection Service, *TCS Credit Reports* (2006) <www.tascol.com.au/reports.htm> at 5 May 2008.

8 Veda Advantage, *Discover Your Credit History* (2005) <www.mycreditfile.com.au> at 5 May 2008.

included in the file.[9] It has been suggested that individuals should check their credit reports periodically to protect themselves against the consequences of credit fraud.[10]

59.13 Veda Advantage advised that the annual rate of consumer access to its credit reporting information is 1.5%, compared to 2.9% in the United Kingdom and 8.2% in the United States. Veda stated that its 'long term objective' is to lift this public access rate to 10%. It noted, however, that

> There are significant business impediments to achieving that goal. The online consumer access and straight through processing required to achieve the goal is impeded by the current law. Current negative credit files contain insufficient information to conclusively identify a consumer. As a result, additional documentary information is required for 19% of file access requests resulting in significant additional handling costs. This circumstance will be improved if comprehensive reporting data is permitted.[11]

Discussion Paper proposal

59.14 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide individuals with rights to obtain access to and correct credit reporting information based on the provisions currently set out in ss 18H and 18J of the *Privacy Act*.[12] The ALRC also asked whether the new regulations should provide that individuals have the right to obtain a free copy of their credit reporting information.[13]

Submissions and consultations

59.15 Stakeholders agreed, in principle, with the ALRC's proposal that the access and correction provisions in the new regulations be based on the provisions currently set out in ss 18H and 18J.[14]

59.16 Galexia Pty Ltd (Galexia) submitted that access provisions should be contained in the new regulations, rather than an industry code, because access is a 'rights' matter rather than an operational issue. Galexia accepted, however, that some 'detailed

---

9 Veda Advantage, *My Veda Alert* (2006) <www.mycreditfile.com.au> at 5 May 2008.

10 Australasian Consumer Fraud Taskforce, *Scams Target You: Protect Yourself*, 31 January 2007.

11 Veda Advantage, *Submission PR 498*, 20 December 2007.

12 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–1.

13 Ibid, Question 55–1.

14 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

industry processes' to deliver the outcome of free and timely access might need to be included in the credit reporting code of conduct.[15]

59.17 The OPC stated that the new access and correction provisions should clarify the extent to which the 'Access and Correction' principle applies to credit reporting information and to the broader category of 'credit worthiness information'—that is, the information now covered by s 18N of the *Privacy Act*.[16]

59.18 The Australian Finance Conference (AFC) submitted that, in this context, NPP 6 currently provides for 'higher compliance requirements' than under ss 18H and 18J,[17] and that any regulation dealing with access and correction should operate only to the extent that the 'Access and Correction' principle is inadequate.

59.19 More generally, stakeholders referred to the importance of promoting individual access to credit reporting information in ensuring data quality and making the credit reporting system more transparent to consumers.[18] One way to address the absence of a 'sense of ownership' of credit reporting information is to encourage individual awareness of the credit reporting system and the content of their credit reporting information. Stakeholders suggested that educational programs to inform consumers about the operation of the credit reporting system—including how to obtain access to, and correction of, credit reporting information—should be pursued by industry and government, in consultation with consumer groups.[19]

Charging for access

59.20 Stakeholders generally agreed that individuals should have the right to obtain a free copy of their credit reporting information, which was seen as crucial in promoting the exercise of access rights.[20]

---

15 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007. Also Veda Advantage, *Submission PR 498*, 20 December 2007.

16 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. In Ch 57, the ALRC recommends that there should be no equivalent in the new regulations of s 18N, which limits the disclosure by credit providers of personal information in 'reports' related to credit worthiness: s 18N(9). See Rec 57–6.

17 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

18 Veda Advantage, *Submission PR 272*, 29 March 2007; Westpac, *Submission PR 256*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Edentiti, *Submission PR 210*, 27 February 2007.

19 Westpac, *Submission PR 256*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 3.

20 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Galexia Pty Ltd, *Submission PR 465*, 13 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail

59.21 The Consumer Action Law Centre stated that credit reporting information is 'important personal information and every person should have free access in order to ensure it is accurate and fair' and noted that the *Credit Reporting Act 1978* (Vic) provides for a right of access to a credit report at no cost.[21] The Consumer Credit Legal Centre (NSW) (CCLC) recommended that credit reporting agencies be obliged to provide a free copy of an individual's credit report to that individual and to 'publicise prominent information about how to get a free copy of your credit report'.[22]

59.22 Legal Aid Queensland expressed concern that the 'method and delivery of access' for Veda Advantage's free access service 'appears to unduly restrict access'.[23] Veda Advantage stated that, 'at the request of and in consultation with consumer organisations, Veda has recently improved the ease of access to information about how to request free credit reports online'. Veda also noted that it intends to

> re-engineer its public access infrastructure as it implements a comprehensive reporting system. This will also include re-shaping the basic and value add credit information products available to consumers. Once online access is available, and identity security is assured, it should be possible to provide access to a basic credit report online without any charge.[24]

59.23 The National Australia Bank supported free access but, in recognition of the cost of providing the service, suggested that the obligation be limited to one free copy per year.[25]

59.24 The Australasian Retail Credit Association (ARCA) stated that, if more comprehensive credit reporting were introduced, more consumers would request access to their credit reporting information. ARCA supported the access rights currently provided by the *Privacy Act*, and noted that

> because of limitations of the current law, processes for identifying consumers and providing access to credit information are highly labour intensive and there are limits on how much automation is possible. These processes will be reformed as the law changes. ARCA supports a goal of free access to reports for consumers, including ultimately online, web enabled access, but recommends that the law be non-prescriptive on charging and the detail of access methods, but rather these details be left to the Code of Conduct.[26]

Credit Association, *Submission PR 352*, 29 November 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 3.

21 *Credit Reporting Act 1978* (Vic) s 4.

22 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 4.

23 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

24 Veda Advantage, *Submission PR 498*, 20 December 2007.

25 National Australia Bank, *Submission PR 408*, 7 December 2007.

26 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

59.25 The OPC submitted that the new regulations should provide that

> (a) individuals should be able to obtain access to a free copy of their credit reporting information (which is not limited to circumstances where the request for access relates to refusal of the individual's application for credit or is otherwise related to the management of the individual's credit arrangements); and
>
> (b) credit reporting agencies may only impose a fee for access to credit reporting information or refuse or defer a request for access in limited circumstances (such as where the individual makes an unreasonable number of requests for access, or requests access within a specified short timeframe).[27]

59.26 The OPC also suggested that the regulations specify a timeframe within which a free copy of credit reporting information must be provided.[28] The Financial Counsellors Association of Queensland considered that a maximum of 21 days should be prescribed by regulation.[29] Galexia suggested that, 'to reflect the nature of modern information systems and communication channels', free access should be required to be given quicker than the current 10 working days.[30]

Correction of credit reporting information

59.27 The CCLC expressed concern about the drafting of s 18J, which deals with the correction of credit reporting information. Section 18J(2) provides for the inclusion of a statement on the credit information file or credit report in circumstances where the credit reporting agency 'does not amend' the information in accordance with an individual's request. The CCLC submitted that:

> This poor drafting effectively provides no incentive for the credit reporting agency to comply with the requirement of ensuring that the credit report is accurate. In practice, all that the credit reporting agency is required to do under this section is to include a statement of the amendment sought and to notify people nominated by the individual of the amendment made, if any, or the statement of the amendment sought.[31]

59.28 The Cyberspace Law and Policy Centre noted concerns that s 18J does not 'expressly require correction rather than mere annotation'. It suggested that, for the avoidance of doubt, the law should be amended to require correction where it is objectively determined that information is inaccurate, out-of-date, incomplete or misleading.[32]

---

27 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
28 Ibid.
29 Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.
30 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.
31 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28*, 6 June 2006.
32 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007. Also Australian Privacy Foundation, *Submission PR 275*, 2 April 2007.

59.29 The role of correcting statements (sometimes referred to as 'notations') raises a number of concerns. Veda Advantage submitted that the regulations should not allow for consumer notations to be included in credit reporting information. As noted in Chapter 57 (in relation to identity theft), notations may have limited practical effect.[33]

> Almost no credit provider ever sees a physical credit report. Rather, credit reporting information is provided as a data stream to a credit provider, which normally processes it in an automated system. As a result, the continuing provision for file statements, used in the event that a consumer is not satisfied by a dispute resolution, is ineffective and misleading for consumers. Rather, Veda supports stronger dispute resolution procedures, including a reversal of the onus of proof, to provide more effective outcomes for consumers.[34]

59.30 Other stakeholders suggested that the practical effect, if notations are not taken into account by automated credit systems, may be that credit reporting information reported to credit providers may not be 'accurate, up-to-date, complete and not misleading' in terms of s 18J.[35] The Australian Privacy Foundation submitted that one solution is to 'mandate' the use of notations by automated systems.[36]

59.31 The OPC stated that new access and correction provisions should clarify the relationship between the obligations on credit providers and credit reporting agencies to make or note corrections requested by an individual and to substantiate disputed credit reporting information.[37]

ALRC's view

Access to credit reporting information

59.32 The new *Privacy (Credit Reporting Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model UPPs.[38] The obligations to provide individuals with access to credit reporting information under s 18H(1) and (2) broadly duplicate the obligations provided by the 'Access and Correction' principle in the model UPPs. Crucially, however, s 18H is not subject to the plethora of exceptions provided for in the 'Access and Correction' principle.[39] There was no suggestion that access to credit reporting information should be subject to any similar exceptions.

59.33 The new *Privacy (Credit Reporting Information) Regulations*, like Part IIIA, will not require that an individual consent to disclosure of information by a credit provider to a credit reporting agency. Individuals will have limited ability to control the

---

33 Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

34 Veda Advantage, *Submission PR 498*, 20 December 2007.

35 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

36 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

37 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

38 Rec 54–2.

39 See Ch 29.

subsequent use or disclosure of credit reporting information. In this context, it is essential that individuals' access to credit reporting information about them should be promoted.

59.34 Individuals should have unfettered rights of access to their credit reporting information. This dictates that the new regulations should provide separately for individual access, and not rely on the UPPs.

59.35 In addition, the issue of charging for access to credit reporting information needs to be dealt with in regulations. The major credit reporting agencies already provide credit reporting information free of charge to the individuals concerned. In general, the ALRC's understanding is that access to credit reporting information is being facilitated adequately. The new *Privacy (Credit Reporting Information) Regulations* should ensure that this continues by providing that individuals have a right to obtain at least one free copy of their credit reporting information annually. Beyond that, the 'Access and Correction' principle in the model UPPs will ensure that any charge is not excessive.

Correction of credit reporting information

59.36 The correction provisions of s 18J of the *Privacy Act* need not be incorporated in the new *Privacy (Credit Reporting Information) Regulations* because to do so would duplicate provisions of the 'Access and Correction' principle.

59.37 In both cases, reasonable steps must be taken to correct information so that it is accurate, complete, up-to-date and not misleading. The 'Access and Correction' principle contains an additional requirement that information be 'relevant'. This additional requirement will have no significant operation in the credit reporting context as the new regulations will prescribe the permissible content of credit reporting information.

59.38 Section 18J and the 'Access and Correction' principle also contain similar provisions dealing with correcting statements. A key difference, however, is that the principle contains a provision obliging an agency or organisation to notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances. There seems no reason why this should not apply to credit reporting information, where it is generally practicable for a credit reporting agency to send correcting information to credit providers to whom inaccurate information previously has been sent.

Recommendation 59–1 The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to obtain access to credit reporting information based on the provisions currently set out in s 18H of the *Privacy Act.*

Recommendation 59–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must provide individuals, on request, with one free copy of their credit reporting information annually.

Third party access

59.39 Part IIIA places some specific constraints on direct access to credit reporting information by persons authorised by the individual. Section 18H(3) of the *Privacy Act* states that an individual's rights of access under the section

> may also be exercised by a person (other than a credit provider, mortgage insurer or trade insurer) authorised, in writing, by the individual to exercise those rights on the individual's behalf in connection with:
>
> (a) an application, or a proposed application, by the individual for a loan; or
>
> (b) the individual having sought advice in relation to a loan.

59.40 In DP 72, the ALRC asked whether the new regulations should provide an equivalent of s 18H(3), so that an individual's rights of access to credit reporting information may be exercised by a person authorised in writing and for a credit-related purpose.[40]

59.41 A related issue concerns whether the access rights provided by s 18H may be used as a 'backdoor' means of indirect access by entities prohibited from obtaining credit reports.[41] Employers, insurers or government agencies, for example, might request individuals to provide copies of their credit reporting information for employment, insurance, licensing or other purposes unrelated to the provision of credit.[42]

59.42 In DP 72, the ALRC stated that there was no need for any new legislative provision prohibiting the collection of an individual's credit reporting information by third parties (that is, persons other than the individual, credit reporting agency or a

---

40 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 55–2.

41 G Greenleaf, 'The Most Restrictive Credit Reference Laws in the Western World?' (1992) 66 *Australian Law Journal* 672, 674.

42 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 36.

credit provider for credit-related purposes), such as employers, insurers or government agencies, through the individual concerned.[43]

Submissions and consultations

59.43 Some stakeholders agreed that it would be desirable to include an equivalent of s 18H(3) in the regulations.[44] The OPC supported including an equivalent of s 18H(3), and submitted that, in developing such a provision, consideration should be given to:

> (a) providing for appropriate exemptions to the requirement that an authorisation be in writing, if necessary for the provision of speech to speech relay services; and
>
> (b) options for restricting the categories of persons or entities that are able to be authorised by the individual.[45]

59.44 Other stakeholders expressed concern that restrictions on access by third parties might create difficulties for credit providers and their customers. The Mortgage and Finance Association of Australia, for example, stated:

> It is important that agents for borrowers can obtain the information, without prescribing that those agents need any specific qualifications (ie they do not need to be lawyers, financial planners, finance brokers etc).[46]

59.45 Legal Aid Queensland observed that it is

> important that individuals are able to request copies of their reports through advocacy, financial counselling and consumer agencies as well as the consumer's legal representative and that that access is not unduly restricted.[47]

59.46 The AFC noted that credit providers may need to discuss credit commitments with non-English speaking customers over the telephone through an English speaking intermediary; or with hearing or speech-impaired customers using the National Relay Service (NRS).[48] The AFC stated that:

> The current credit reporting provisions prevent the credit provider from discussing the customer's credit commitments with a third party without the 'written' authorisation of the customer. While verbal or implicit consent is permitted in other provisions of the Act, written consent only is permissible in this instance.[49]

---

43 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.31].

44 GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

45 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

46 Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

47 Legal Aid Queensland, *Submission PR 489*, 19 December 2007

48 The NRS is discussed further in Ch 70.

49 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

59.47 The AFC submitted that authority to access credit reporting information should not need to be in writing, but be based on the implied or express consent of the individual concerned. The AFC also questioned the desirability of restricting access for a 'credit-related purpose'.

> Given access must be with the individual's authorisation, we see no reason why these third parties should not be able to directly obtain a copy of the report and use for the reason the authorisation was obtained.[50]

59.48 Other stakeholders also considered that there should be less restriction on individuals providing access to their credit reporting information to third parties. The Institute of Mercantile Agents referred to

> a growing trend, especially by larger employers such as multi-nationals concerned about the prospects of fraudulent behaviour and seeing the provision of credit histories as a positive identification step. Similarly, insurers may well be keen in the face of a suspicious claim say for a vehicle theft or fire damage of premises to require a claimant to produce his/her personal credit history … If there are legitimate grounds for access, especially when initiated by the individual concerned, then access ought to be granted—with the credit history information recorded, the ability to provide low cost access should be not be at all difficult or onerous.[51]

59.49 Some stakeholders supported including an equivalent of s 18H(3) in the new regulations, but submitted that credit reporting regulation, and the *Privacy Act* generally, should be drafted to prevent 'forced' or 'coerced' access for the purposes of third parties.[52] The CCLC recommended that an offence should be created under the *Privacy Act* to prevent persons from 'requiring an individual to provide a copy of his/her credit report in the course of any business or enterprise'.[53]

59.50 The OPC recommended that it provide guidance on practices that require individuals to provide copies of their credit reports for any purpose unrelated to the provision of credit. It also suggested that review of the new regulations[54] include 'further consideration of the need for an express provision prohibiting the collection of an individual's credit information file by employers, insurers and government agencies'.[55]

ALRC's view

59.51 As discussed in Chapter 70, there is nothing in the *Privacy Act* that prevents an individual from providing consent for an agency or organisation to disclose information to a third party. While there are concerns that such consensual

---

50 Ibid.

51 Institute of Mercantile Agents, *Submission PR 270*, 28 March 2007.

52 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

53 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 36.

54 Rec 54–8.

55 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

arrangements are not implemented consistently or recognised by agencies and organisations, there is no requirement that consent be in writing or any limitation placed on the purposes for which information may be disclosed, with consent, to a third party.

59.52 The ALRC does not recommend any change to the *Privacy Act* with regard to third party access with consent.[56] Rather, the ALRC considers that guidance is the most appropriate way to deal with problems about consensual third party arrangements and recommends that the OPC develop and publish guidance on third party representatives.[57]

59.53 Section 18H(3) requires authorisation in writing and limits the purposes for which an individual's access rights may be exercised by another person. This may be seen as contrary to the more flexible policy approach adopted by the ALRC in relation to third party access more generally.

59.54 In the ALRC's view, however, the privacy risks involved with credit reporting information—including, for example, the risk of identity fraud—justify the more stringent approach. The fact that there may be pressure on individuals to consent to third party access—for example, by employers, insurers or government agencies— is another reason to adopt this approach.

59.55 The ALRC is not convinced, however, that there is any need for new legislative provisions prohibiting individuals from being required to provide their credit reporting information for non-credit related purposes. The collection of credit reporting information for non-credit related purposes should be regulated adequately by the 'Collection' principle in the model UPPs (that is, collection must be 'necessary' for one or more of an organisation's or agency's functions or activities).[58]

59.56 An equivalent of s 18H(3) would not prevent third parties—such as the NRS—providing assistance to individuals in communicating with credit providers or credit reporting agencies. A distinction should be made between circumstances in which a third party is assisting the individual to obtain access, and where the third party is seeking to obtain access to information directly from the credit provider or credit reporting agency for their own purposes. In the former case, the third party is not, in terms of s 18H(3), exercising rights of access 'on the individual's behalf', but is assisting the individual to exercise those rights themselves. This is a matter that could be dealt with by OPC guidance.

---

56 The ALRC does recommend, however, that the *Privacy Act* be amended to provide for nominee arrangements establishing long term recognition of nominated substitute decision makers: Recs 70–1, 70–2.

57 Rec 70–3.

58 Rec 21–5.

Recommendation 59–3 The new *Privacy (Credit Reporting Information) Regulations* should provide an equivalent of s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised for a credit-related purpose by a person authorised in writing.

Notification of adverse credit reports

59.57 Under s 18M of the *Privacy Act*, when an individual's application for credit is refused, based wholly or partly on a credit report, the credit provider must give the individual written notice of that fact and advice about the individual's right to obtain access to his or her credit information file held by the credit reporting agency.

59.58 Neither the NPPs nor the model UPPs contain an equivalent provision. Section 18M is essential, however, for the operation of Part IIIA of the *Privacy Act*. Unless an individual is made aware that the reason credit has been refused is due to credit reporting information received by the credit provider, the individual will not be in a position to obtain access to that information, check the accuracy of the information or seek its correction.

59.59 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide individuals with rights to be notified about adverse credit reports, based on the provisions currently set out in s 18M.[59] Stakeholders who addressed the issue all agreed with the ALRC's proposal,[60] which is confirmed in the recommendation below.

Recommendation 59–4 The new *Privacy (Credit Reporting Information) Regulations* should provide that, where a credit provider refuses an application for credit based wholly or partly on credit reporting information, it must notify an individual of that fact. These notification requirements should be based on the provisions currently set out in s 18M of the *Privacy Act*.

---

59 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–2.

60 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

Information about credit scoring processes

59.60 In DP 72, the ALRC noted that there may be reasons for credit being refused that are based on credit reporting information, but are not readily apparent from the information received by the credit provider or provided to the individual concerned.[61]

59.61 Where this is the case, notification of an adverse credit report under s 18M, or an equivalent provision in the new *Privacy (Credit Reporting Information) Regulations*, may not achieve the intended policy result. That is, even where the individual concerned obtains access to the credit reporting information, he or she may not be able to understand why that information contributed to credit being refused.

59.62 An example of such circumstances is where credit reporting information is used in credit scoring. Credit scoring may be described as the use of 'mathematical algorithms or statistical programmes that determine the probable repayments of debts by consumers, thus assigning a score to an individual based on the information processed from a number of data sources'.[62] A range of different data items, derived from credit reporting information or from a credit provider's own records, may be used in credit scoring.

59.63 If an individual is refused credit based on a credit score, this fact will not be apparent from the credit report. A credit score is not permitted content of a credit information file under s 18E.[63] Further, credit reporting agencies and credit providers may rely on the 'evaluative information' exception in NPP 6.2 (retained in the 'Access and Correction' principle in the model UPPs),[64] to avoid giving individuals credit scores or rankings and instead provide an explanation.[65]

59.64 In response to the Issues Paper, *Review of Privacy–Credit Reporting Provisions* (IP 32), the Australian Privacy Foundation submitted that

> there should be a clear statutory right of access to credit scores and other rankings held by [credit reporting agencies] and [credit providers], together with explanatory material on scoring systems and current thresholds for acceptance, to allow individuals to better understand how they are being assessed.[66]

---

61 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.44].

62 F Ferretti, 'Re-thinking the Regulatory Environment of Credit Reporting: Could Legislation Stem Privacy and Discrimination Concerns' (2006) 14 *Journal of Financial Regulation and Compliance* 254, 261. See Ch 52.

63 New Zealand credit reporting regulation permits credit reporting information to include a credit score: *Credit Reporting Privacy Code 2004* (NZ) cl 5, definition of 'credit information'.

64 UPP 9.2.

65 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007. See also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007.

66 Australian Privacy Foundation, *Submission PR 275*, 2 April 2007. See also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007.

59.65 In DP 72, the ALRC noted that, in the United States, the *Fair Credit Reporting Act 1970* (US) (FCRA) requires credit reporting agencies to provide, on request, prescribed information to individuals about the use of credit scoring.[67] The FCRA provides:

> (1) *In general.* Upon the request of a consumer for a credit score, a consumer reporting agency shall supply to the consumer a statement indicating that the information and credit scoring model may be different than the credit score that may be used by the lender, and a notice which shall include—
>
> (A) the current credit score of the consumer or the most recent credit score of the consumer that was previously calculated by the credit reporting agency for a purpose related to the extension of credit;
>
> (B) the range of possible credit scores under the model used;
>
> (C) all of the key factors that adversely affected the credit score of the consumer in the model used, the total number of which shall not exceed four …
>
> (D) the date on which the credit score was created; and
>
> (E) the name of the person or entity that provided the credit score or credit file upon which the credit score was created.[68]

59.66 In DP 72, the ALRC observed that, while providing rights of access to actual credit scores would not serve any useful purpose, the provision of explanatory material about the key factors that adversely affected the credit score of an individual might benefit consumers.[69]

59.67 In the United States, credit reports provided to individuals include information about the factors that affect an individual's credit score adversely (or favourably). For example, a sample Fair Isaacs Corporation 'MyFICO' score summary lists the following as negative factors:

- You have a public record and a serious delinquency on your credit report.
- You have multiple accounts showing missed payments or derogatory descriptions.
- The balances on your non-mortgage credit accounts are too high.

59.68 Factors listed as helping the credit score include:

- You have an established credit history.
- You have an established revolving credit history.
- You currently have a good number of credit accounts.[70]

---

67 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.39].

68 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US), § 1681g(f)(1).

69 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.40].

70 Fair Isaac Corporation, *Sample FICO Score Summary* (2007) <www.myfico.com/Products/FICOOne/Sample/FICOScore/Sample_Summary.aspx> at 5 May 2008.

59.69 The ALRC recognised that, as information relevant to some of these factors is not available from credit reporting agencies under current credit reporting regulation, different factors would apply under Australian credit scoring conditions.[71]

Discussion Paper proposal

59.70 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide that the information to be given, if an individual's application for credit is refused based wholly or partly on credit reporting information, should include any credit score or ranking used by the credit provider, together with explanatory material on scoring systems, to allow individuals to understand how the risk of the credit application was assessed.[72]

Submissions and consultations

59.71 Some stakeholders agreed with the ALRC's proposal.[73] In supporting the proposal, the OPC submitted that the new regulations also should clarify the rights of access and correction that are to apply to credit scores and rankings.[74]

59.72 Credit providers and other industry stakeholders opposed the proposal, at least to the extent that it would require disclosure or detailed explanation of credit scores or rankings.[75] The reason for this opposition included that:

- credit scoring processes involve highly complex and commercially sensitive methodologies, which it would be inappropriate to require organisations to disclose;[76]

---

71 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.43].

72 Ibid, Proposal 55–3.

73 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

74 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

75 GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

76 GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

- credit scoring processes vary significantly over time and between credit providers, making the disclosure and explanation of credit scores or rankings difficult and of limited value to individuals;[77] and

- detailed disclosure of credit scoring processes increases the risk of manipulated or fraudulent credit applications.[78]

59.73 ARCA agreed that there needs to be greater transparency with regard to the use of scoring in credit assessment, but stated that, in practice, there would be problems with providing detailed information.

> Unlike the US where a single model is used to determine credit scores there is no uniform score in Australia. Different institutions use different models which represent highly complex proprietary information that differs between them, and even between different parts of a single institution.[79]

59.74 Stakeholders referred to variations in the credit scoring processes used by credit providers and credit reporting agencies. Optus stated that

> providing the customer with a credit score or ranking will be meaningless, especially in the absence of a common scoring or ranking system, as per the American FICO score, which (as we understand it) is provided by the credit reporting agency, not the credit provider.[80]

59.75 The ANZ submitted that the ALRC's proposal would not make individuals better informed about how the risk of their credit application was assessed, because

> financial institutions have developed proprietary systems which rely on criteria specific to the organisations' own credit assessment requirements. Many of these systems do not use the same terminology or the same scale for assessing customer scores. Therefore, knowing a score with one organisation is likely to serve only as a guide to whether or not the individual would (or would not) obtain credit from another organisation.[81]

---

77 Optus, *Submission PR 532*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

78 GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

79 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

80 Optus, *Submission PR 532*, 21 December 2007. The AFC stated that, in any case, credit scores are not generally retained on the records of a credit reporting agency or credit provider beyond the time a credit application is approved or declined: Australian Finance Conference, *Submission PR 398*, 7 December 2007.

81 ANZ, *Submission PR 467*, 13 December 2007.

59.76 GE Money Australia (GE Money) expressed concern that 'explaining how to get a better credit score is more likely than not to increase the incidence of data manipulation by applicants for credit'.[82] Similarly, the AFC stated that

> a requirement to disclose components of an application that are taken into account to arrive at a credit score would potentially enhance the opportunity for information manipulation by a customer or intermediary and inappropriately increase credit risk for the industry.[83]

59.77 GE Money noted that, in its view, one of the benefits of moving to more comprehensive credit reporting would be that 'the numerous proprietary credit scoring systems will converge into a single credit scoring system that can be disclosed to consumers, and the incidence of applicant data manipulation can be dramatically decreased'.[84]

59.78 The OPC provided a different perspective on industry objections to the ALRC's proposal. The OPC recognised that 'there is significant complexity in credit scoring systems, and a range of data items other than credit reporting information may be used in creating an individual's credit score or ranking'. It stated that individuals should still have the opportunity to compare credit scores against credit reporting information as this may provide them with 'a general indication of whether they might want to request access to other personal information about them that is held by the credit reporting agency or credit provider'.[85]

59.79 Many stakeholders that opposed the ALRC's proposal in DP 72 nevertheless favoured imposing an obligation to provide some form of 'generic' explanation about credit scoring.[86] ARCA, for example, stated that it would support credit providers giving individuals 'a brief description, in plain English, of standard credit scoring and an explanation of how this may have been used in the credit decision'.[87]

Other information provided on refusal of credit

59.80 In DP 72, the ALRC noted that, apart from credit scoring, there may be other reasons for credit being refused that are based on credit reporting information, but are not necessarily apparent from an individual's access to his or her credit report.[88] The CCLC submitted, for example, that:

---

82 GE Money Australia, *Submission PR 537*, 21 December 2007.

83 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

84 GE Money Australia, *Submission PR 537*, 21 December 2007.

85 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

86 Veda Advantage, *Submission PR 498*, 20 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

87 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007. See also National Australia Bank, *Submission PR 408*, 7 December 2007.

88 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.44].

> The law should be clarified to ensure that individuals who are refused credit on the basis that their file has been cross-referenced to another file, or any other reason that is based on information held by a credit reporting agency that is not apparent from the copy of the file the individual would be given upon request, are entitled to be given adequate information to enable them to correct any inaccuracies or false assumptions attributable to the data held by the credit reporting agency.[89]

59.81 The OPC submitted that individuals should be given access to adequate information to enable them to correct any inaccuracies or false assumptions attributable to the information held by the credit reporting agency or credit provider.

> For example, information about the linking of the individual's credit file to another file should be provided to an individual, either as part of the refusal notification or as part of access to his or her credit information file.[90]

59.82 The OPC stated that the provision of adequate information where refusal of credit is notified would be consistent with the general obligation on credit providers and credit reporting agencies to take reasonable steps to ensure the credit reporting information held is accurate, complete, up-to-date and not misleading. The OPC suggested that it provide guidance on the additional information to be provided to individuals in a refusal notification to promote and maintain data accuracy. It stated that this additional information 'could include explanatory material on practices in relation to the linking of credit information files and reviews of automated decisions'.[91]

59.83 Concerns about the linking of credit information files generally also are discussed in Chapter 58. The ALRC recommends that the credit reporting industry code[92] should promote data quality by setting out procedures dealing with, among other things, the linking of credit reporting information.[93]

ALRC's view

59.84 The ALRC's proposal, in DP 72, that new regulations require the provision by credit providers of information about credit scoring was influenced by the FCRA model. There are, however, important differences between credit scoring practices in the United States and Australia, which were not fully appreciated.

59.85 Australian credit scoring systems (or 'scorecards') are relatively more dependent for their predictive power on internal credit provider data, derived from application forms and information about existing customers, as opposed to information from credit reporting agencies. These scorecards vary significantly and are considered commercially sensitive. In contrast, the comprehensive information held by United States credit reporting agencies, and the dominant position of companies (such as the

---

89 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 23.

90 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

91 Ibid. Automated decision review mechanisms are discussed in Ch 10.

92 Rec 54–9.

93 Rec 58–3.

Fair Isaacs Corporation) that provide credit scoring systems based on this information, have led to more uniformity in credit scoring practices.

59.86 These differences mean that imposing detailed obligations to provide prescribed information to individuals about the use of credit scoring, as in the United States, may not be appropriate or practicable. From one perspective, a lower degree of transparency in relation to credit decisions is one price that must be paid for not having moved to a more comprehensive credit reporting system.

59.87 It is important that, when an individual's application for credit is refused, adequate information is provided to enable the individual to correct any inaccuracies or false assumptions attributable to the personal information held by the credit reporting agency or credit provider. This outcome would be assisted by a general explanation of the use of credit scoring processes.

59.88 In light of the practical difficulties referred to above, however, it would not be appropriate for the new *Privacy (Credit Reporting Information) Regulations* to mandate the provision of prescribed information about credit scoring. The provision of information, including about credit scoring, on refusal of credit is an appropriate subject for OPC guidance.

Complaint handling

59.89 The following section of this chapter examines aspects of complaint handling in relation to credit reporting. Complaints about credit reporting are handled by credit reporting agencies and credit providers, external dispute resolution (EDR) schemes such as the Telecommunications Industry Ombudsman (TIO) and Banking and Financial Services Ombudsman (BFSO),[94] or by the OPC under the complaint-handling provisions of the *Privacy Act.*

Credit reporting agencies and credit providers

59.90 Under the *Credit Reporting Code of Conduct*, credit reporting agencies and credit providers must establish procedures to deal with disputes relating to credit reporting.[95] Credit providers that are financial services providers under the *Corporations Act 2001* (Cth) are required to establish internal dispute resolution systems that comply with standards set by the Australian Securities and Investments Commission (ASIC).[96] Internal dispute resolution systems also may be required by

94 In October 2007, the BFSO announced that it would merge with the Financial Industry Complaints Service and the Insurance Ombudsman Service. The new EDR scheme is expected to operate from 1 July 2008: Banking and Financial Services Ombudsman, 'EDR Scheme Merger' (Press Release, 30 October 2007).

95 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), Part 3.

96 *Corporations Act 2001* (Cth) s 912A(2)(a).

industry codes, such as the *Code of Banking Practice*[97] or by the terms of membership of EDR schemes.

59.91 The *Credit Reporting Code of Conduct* makes credit reporting agencies responsible for attempting to resolve disputes between credit providers and individuals where the dispute involves the content of a credit report. The Code states:

> 3.3 A credit provider should refer to a credit reporting agency for resolution a dispute between that credit provider and an individual where the dispute concerns the contents of a credit report issued by the credit reporting agency.
>
> 3.4 In referring a dispute to a credit reporting agency, a credit provider must inform the individual of the referral and must provide the individual with the name and address of the credit reporting agency.
>
> 3.5 Upon receipt, from a credit provider, of a referral of a request for dispute resolution, a credit reporting agency must handle the request as if the request had been made directly to the agency by the individual concerned.
>
> …
>
> 3.7 Where a credit reporting agency establishes that it is unable to resolve a dispute it must immediately inform the individual concerned that it is unable to resolve the dispute and that the individual may complain to the Privacy Commissioner.[98]

59.92 After receiving a complaint about the content of a credit report, Veda Advantage recommends that the complainant first contact the credit provider responsible for the listing to resolve the issue. If that is unsuccessful, Veda conducts an investigation 'on the consumer's behalf'.[99] Veda Advantage advised that it 'currently manages approximately 25,000 investigations arising from consumer complaints each year'.[100] Veda stated that:

> Approximately 34% of investigations require assistance from our subscribers before they can be resolved … Others involve reference to external parties such as the Insolvency and Trustee Service of Australia … 47% of complaints require minor investigation … or an internal check, usually on data quality issues …[101]

External dispute resolution schemes

59.93 Many credit providers are members of EDR schemes, including financial services providers who are required by the *Corporations Act* to belong to an EDR scheme approved by ASIC.[102]

59.94 ASIC-approved and other EDR schemes deal with some complaints about credit reporting. The TIO, for example, receives and resolves complaints concerning credit

---

97 Australian Bankers' Association, *Code of Banking Practice* (1993).
98 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991).
99 Veda Advantage, *Submission PR 272*, 29 March 2007.
100 Veda Advantage, *Submission PR 498*, 20 December 2007.
101 Veda Advantage, *Submission PR 272*, 29 March 2007.
102 *Corporations Act 2001* (Cth) s 912A(2)(b).

reporting by telecommunications service providers.[103] The TIO advised that, in the six months to December 2006, it received 1,437 complaints concerning credit reporting.[104]

59.95 The BFSO resolves some complaints concerning credit reporting by banks and their affiliates.[105] The BFSO stated that in a five-year period to December 2006, it closed 517 cases where 'privacy' or 'credit reporting' was recorded as a 'problem type'. The BFSO noted, however, that problems with credit reporting commonly arise in the course of disputes about other matters such as debts, and the credit reporting aspect 'is not always captured by the BFSO data collection system if the credit reporting issue is incidental to the main issues in dispute'.[106]

59.96 Other utilities and finance industry ombudsmen—such as the Energy and Water Ombudsman NSW, the Credit Ombudsman Service and the Credit Union Dispute Resolution Centre—may also deal with credit reporting complaints.

The Office of the Privacy Commissioner

59.97 The *Privacy Act* provides an avenue for individuals to complain to the Privacy Commissioner about an act or practice that may be an interference with their privacy.[107] The Act sets out detailed provisions on how the Commissioner can receive, investigate and resolve complaints, including credit reporting complaints.[108] The investigation and resolution of complaints under Part V of the Act is discussed in detail in Chapter 49.

Complaint-handling processes

59.98 A range of criticisms have been made about the handling of credit reporting complaints. These included concerns that:

- in order to initiate a credit reporting complaint with the OPC, complainants may be required to contact the credit reporting agency to obtain a copy of their credit information file and then to complain to the credit provider;[109]

---

103 The TIO is wholly funded by telecommunications service providers, who are required by law to be part of, and pay for, the TIO Scheme: *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 126.

104 Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007.

105 Banking and Financial Services Ombudsman, *Case Studies* <www.abio.org.au> at 5 May 2008. Non-bank institutions and their affiliates can also apply to join the BFSO scheme: Banking and Financial Services Ombudsman, *About Us* <www.abio.org.au> at 5 May 2008.

106 Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007.

107 *Privacy Act 1988* (Cth) s 36(1).

108 Ibid s 6 defines a 'credit reporting complaint' as a complaint about an act or practice that, if established, would be an interference with the privacy of the complainant because: (a) it breached the Code of Conduct; or (b) it breached a provision of Part IIIA.

109 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 139.

- dispute resolution procedures established by credit providers and credit reporting agencies lack transparency and fail to address complaints in relation to repeated problems or possible systemic issues;[110] and

- dispute resolution procedures generally place the onus of proving that listings are inaccurate on individuals who lack any real negotiating power.[111]

The complaints 'merry-go-round'

59.99 Stakeholders emphasised concerns[112] about what has been termed the credit reporting complaints 'merry-go-round'.[113] Section 41(1A) of the Act provides that the Commissioner must not investigate a complaint if the complainant did not complain to the respondent before making the complaint to the Commissioner. Consistently, the *Credit Reporting Code of Conduct* provides that:

> The Privacy Commissioner may decide not to investigate a complaint about a credit reporting dispute if the Commissioner considers that:
>
> (a) the dispute should first be dealt with by a credit reporting agency or credit provider; or
>
> (b) the dispute is being, or has been, dealt with adequately by the credit reporting agency or credit provider.[114]

59.100 Under the *Privacy Act*, the respondent to a complaint is the person who engaged in the act or practice that is the subject of the complaint.[115] In the case of credit reporting complaints, it is often unclear whether the problem has been caused by the credit provider or the credit reporting agency, making the respondent to the complaint hard to identify.[116]

59.101 The Consumer Action Law Centre observed that the most common way in which an individual discovers inaccurate information is when the individual obtains a copy of his or her credit report—usually after an application for a loan has been rejected on the basis of the credit report. This generally means that the consumer makes a complaint to the credit reporting agency. Under the Code, the credit reporting agency must try to resolve the dispute and, where it cannot, it is required to inform the individual concerned that the individual may complain to the OPC (not to the credit provider).

---

110 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.11].

111 Ibid, [5.11].

112 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; National Credit Union Association Inc, *Submission PR 226*, 9 March 2007.

113 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; J Corker and C Bond, 'The Merry-Go-Round: Credit Report Complaint Handling under the Privacy Act' (2001) 8(5) *Privacy Law and Policy Reporter* 1.

114 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [3.17].

115 *Privacy Act 1988* (Cth) s 36(8).

116 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

> Unfortunately, the practice of the OPC upon receipt of these complaints is to … refer the consumer to the relevant credit provider before it will take the complaint, even though the consumer has already complained to the [credit reporting agency] (and the [credit reporting agency] would most likely have dealt with the credit provider in its investigation of the complaint). If the credit provider cannot or does not resolve the complaint, under the Code they must refer it back to the [credit reporting agency] … It is no wonder that many consumers become confused by the process.[117]

59.102 The Consumer Action Law Centre submitted that, while this 'merry-go-round' is made possible by provisions of the *Credit Reporting Code of Conduct*, 'ultimately it occurs because the OPC does not use its discretion to accept complaints … nor accept that a complaint made to a [credit reporting agency] has been made to the respondent'.[118]

Discussion Paper proposal

59.103 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* should provide that:

> (a) credit reporting agencies and credit providers must handle credit reporting complaints in a fair, efficient and timely manner;
>
> (b) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint;
>
> (c) a credit reporting agency should refer to a credit provider for resolution of a complaint about the content of credit reporting information provided to the agency by that credit provider; and
>
> (d) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint it must immediately inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.[119]

59.104 The ALRC also proposed that the new regulations provide that the information to be given, if an individual's application for credit is refused based wholly or partly on credit reporting information, should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.[120]

Submissions and consultations

59.105 The OPC supported the ALRC's complaint-handling proposal, which it noted is generally consistent with the obligations set out in the *Credit Reporting Code of Conduct*. The OPC also noted that the requirement set out in sub-paragraph (c) of the

---

117 Ibid.

118 Ibid.

119 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–4. In the discussion below, this is referred to as the 'ALRC's complaint-handling proposal'.

120 Ibid, Proposal 55–5.

proposal reverses the existing position,[121] but agreed that the credit provider should be the initial point of referral for a complaint about the content of credit reporting information.[122]

59.106 Other stakeholders also generally supported the ALRC's complaint-handling proposal, although some changes of approach were suggested.[123] While no stakeholder disagreed with the ALRC's proposal, the AFC suggested that complaint handling may be addressed better through a code of conduct, than prescribed by regulation.[124]

59.107 ARCA agreed with the ALRC's complaint-handling proposal, and stated that operational detail should be set out in a code of conduct rather than in the new regulations.[125] In this context, ARCA members have each appointed a 'single point of contact' for complaint handling as part of initiatives to improve the timeliness of complaint handling. ARCA stated:

> ARCA credit providers and [credit reporting agencies] collaborate to resolve a consumer complaint if at all possible at the first point of contact or where it needs to be referred to other parties to simplify the process through the use of the single point of contact network. This has improved customer management, reduced 'hand-offs' of customers and supported an 'end to end process'. ARCA is endeavouring to establish a target of a maximum number of consumer contacts in such a situation. This is expected to include a standard of no more than two contacts for a significant proportion.[126]

59.108 More generally, ARCA and its members have been active in developing new policies and procedures for credit reporting complaint handling, in consultation with consumer groups. ARCA has, among other things, established minimum complaint-handling standards, policies and procedures for its members and a process for reviewing and referring systemic complaints to ARCA for guidance and resolution.[127]

59.109 The Consumer Action Law Centre submitted that there are two main weaknesses with the current complaint-handling system.

---

121 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [3.3].

122 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

123 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; HBOS Australia, *Submission PR 475*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

124 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

125 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

126 Ibid.

127 Ibid. Veda Advantage stated the 'the appropriate place for monitoring and correcting any emerging systemic issues should be the ARCA Policy and Compliance Committee, independently chaired and comprising equal numbers of consumer and industry representatives': Veda Advantage, *Submission PR 498*, 20 December 2007.

> Firstly, the complaints handling process is fragmented, requiring consumers to make more than one complaint to more than one organisation. Secondly, the [OPC's] role as complaints handler is not effective for consumers, nor does it appear to effectively identify systemic problems or gaps in industry complaints handling.[128]

59.110 The Centre generally supported proposals for complaint handling put forward by ARCA and 'ARCA's commitment to a maximum of two consumer contacts in relation to a dispute'.[129] The Centre also proposed, among other things, that credit reporting agencies should have 'an obligation to communicate with the credit provider about the dispute, rather than referring the consumer to the credit provider'. It also proposed that consideration be given to establishing a central register (probably within a credit reporting agency) that would allow credit providers or credit reporting agencies 'to log that a complaint had been made, so that the other party is aware of the complaint'.[130]

59.111 Similarly, Legal Aid Queensland stated that once a complaint is made to a credit reporting agency about a listing, the agency

> should be the intermediary that deals with the credit provider and, if the complaint is not resolved, advises the complainant how to complain to the EDR scheme or the OPC.[131]

59.112 Veda Advantage stated that it supported that ALRC's proposals for dispute resolution generally, 'with some further modifications to strengthen and streamline dispute resolution'. These modifications should include providing that a

> [credit reporting agency] that receives a complaint must do all that is necessary to determine that complaint itself, including contacting credit providers and debt collectors on behalf of the consumer … [132]

59.113 Inaccuracies may exist in credit reporting information acquired from public registers, such as the National Personal Insolvency Index.[133] Veda stated that where it has correctly recorded the public register information it is, nevertheless,

> prepared to consider handling the complaint on behalf of the consumer with the public register owner to ensure the consumer is not 'shopped around'. Detailed consideration of this will be undertaken with consumer advocates.[134]

---

128 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

129 Ibid.

130 Ibid. The Centre stated that this may also assist credit reporting agencies to 'identify possible systemic problems'.

131 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

132 Veda Advantage, *Submission PR 498*, 20 December 2007.

133 The National Personal Insolvency Index is established and maintained in accordance with the *Bankruptcy Regulations 1996* (Cth) pt 13.

134 Veda Advantage, *Submission PR 498*, 20 December 2007.

59.114 Finally, stakeholders agreed with the ALRC's proposal[135] that the new regulations provide that, where an individual's application for credit is refused based wholly or partly on credit reporting information, the information to be given by the credit provider should include information about the avenues of complaint available.[136]

ALRC's view

59.115 Under the existing *Credit Reporting Code of Conduct*, credit reporting agencies are responsible for resolving disputes between consumers and credit providers.[137] Notably, the Code provides that 'a credit provider should refer to a credit reporting agency for resolution a dispute between that credit provider and an individual where the dispute concerns the contents of a credit report issued by the credit reporting agency'.[138]

59.116 A focus on complaint handling by credit reporting agencies may be seen as 'logical given their central role in the credit reporting system',[139] but creates problems in practice. First, where a credit provider considers that information it disclosed to the agency is accurate, the credit reporting agency has limited capacity to 'look behind' the listing of its subscriber credit provider. Arguably, credit reporting agencies cannot resolve credit reporting complaints that require a determination of rights in specific consumer credit contexts. Secondly, an agency's commercial interests may conflict with the need to make decisions that may affect adversely the interests of its subscribers.

59.117 Credit reporting agencies should refer complaints about the content of credit reporting information provided to the agency by a credit provider to that credit provider for initial dispute resolution. As currently set out in the explanatory notes to the Code, and as agreed by the industry, credit reporting agencies should be able to nominate an officer at each credit provider as the first point of contact for the handling of credit reporting complaints.[140]

59.118 Credit reporting agencies and credit providers need to establish effective complaint-handling mechanisms. In many instances, the involvement of a credit reporting agency and a credit provider will be necessary to deal with a credit reporting complaint. The credit provider may need, for example, to investigate the circumstances

---

135 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–5.

136 GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

137 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [3.3]–[3.6].

138 Ibid, [3.3].

139 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

140 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [78B].

of an overdue payment and the credit reporting agency to amend its credit reporting information following the outcome of an investigation. Where credit reporting agencies and credit providers share the handling of a complaint, some potential for a complaint-handling 'merry-go-round' may remain.

59.119 This problem may be addressed, in part, by the provision of appropriate information to complainants about the respective roles of credit reporting agencies and credit providers, and access to EDR and OPC complaint-handling processes.

59.120 The ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* provide that notification of adverse credit reports include information about the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information. In addition, the 'Notification' principle in the model UPPs also will require that, at or before the time credit reporting information is collected, reasonable steps must be taken to notify or ensure that the individual is aware of the fact that avenues of complaint are set out in the agency or organisation's Privacy Policy.[141]

59.121 Time limits on substantiating disputed credit reporting information and mandated credit provider membership of EDR schemes (discussed below) should also help to ensure effective complaint handling for individuals who are contesting adverse credit reporting information.

Recommendation 59–5 The new *Privacy (Credit Reporting Information) Regulations* should provide that:

(a) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint in a fair, efficient and timely manner;

(b) a credit reporting agency should refer to a credit provider for resolution complaints about the content of credit reporting information provided to the agency by that credit provider; and

(c) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint, it must inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

141 See Ch 23.

Recommendation 59–6 The new *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given, if an individual's application for credit is refused based wholly or partly on credit reporting information, should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.

External dispute resolution

59.122 Many credit providers are already members of industry-based EDR schemes, notably those involving the BFSO and TIO. Veda Advantage, the main consumer credit reporting agency, also is a member of the BFSO.[142]

59.123 In 2007, the House of Representatives Standing Committee on Economics, Finance and Public Administration considered the operation of EDR schemes in the context of a report on home loan lending. The Committee concluded that EDR schemes 'appear to be an effective and low-cost mechanism for resolving consumer complaints'.[143] In recommending that the Australian Government regulate credit products, the Committee referred to the fact that membership of an approved EDR scheme is mandatory under the *Corporations Act*.[144]

Discussion Paper proposal

59.124 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide that credit providers only may list overdue payment information where the credit provider is a member of an EDR scheme approved by the OPC.[145]

Submissions and consultations

59.125 In response to IP 32, stakeholders emphasised the desirability of access to EDR schemes in credit reporting complaint handling.[146] The Consumer Action Law

---

142 Other credit reporting agencies are not members of an EDR scheme.

143 Parliament of Australia—House of Representatives Standing Committee on Economics Finance and Public Administration, *Home Loan Lending: Inquiry into Home Loan Lending Practices and the Processes Used to Deal with People in Financial Difficulty* (2007), 48.

144 Ibid, 48–49, rec 2.

145 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–6.

146 Legal Aid Queensland, *Submission PR 292*, 11 May 2007; ANZ, *Submission PR 291*, 10 May 2007; Queensland Law Society, *Submission PR 286*, 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007; National Legal Aid, *Submission PR 265*, 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007; Westpac, *Submission PR 256*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; MasterCard Worldwide, *Submission PR 237*, 13 March 2007; GE Money Australia, *Submission PR 233*, 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd,

Centre, for example, noted that encouraging EDR in credit reporting complaint handling is 'consistent with developments in other industry areas, especially related areas such as financial services regulation and more recently, moves to implement such a requirement in the consumer credit arena'.[147]

59.126 Stakeholders generally supported the proposal made by the ALRC in DP 72.[148] The Uniform Consumer Credit Code Management Committee (UCCCMC) stated that the proposal was consistent with the intention of the Ministerial Council on Consumer Affairs to promote consumer access to EDR in relation to credit disputes. Further, the UCCCMC noted that,

> in not recommending the establishment of a new specialised EDR scheme to handle credit reporting complaints, the proposal also reflects the current trend towards rationalisation of industry-based EDR schemes.[149]

59.127 The Financial Counsellors Association of Queensland stated:

> From our experience, where EDR is working there is a very good chance of a reasonable outcome for the consumer. EDR schemes are only costly to those who choose to disregard due process and push the boundaries of the law.[150]

59.128 A number of industry stakeholders suggested that it would be preferable for EDR schemes to be approved by ASIC, rather than by the OPC (as proposed by the ALRC).[151] The OPC agreed that the new regulations should provide that credit providers only may list overdue payment information where the credit provider is a member of a recognised EDR scheme, but did not support a role for the OPC in 'approving' such schemes.

Submission PR 232, 9 March 2007; Energy and Water Ombudsman NSW, *Submission PR 225*, 9 March 2007; Australasian Retail Credit Association, *Submission PR 218*, 7 March 2007.

147 Consumer Action Law Centre, *Submission PR 274*, 2 April 2007. In 2006, the Victorian Government stated that it supports legislating to require all providers of consumer credit in Victoria to subscribe to an alternative dispute resolution scheme: Victorian Government, *Government Response to the Report of the Consumer Credit Review* (2006), 15.

148 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman, *Submission PR 471*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

149 Uniform Consumer Credit Code Management Committee, *Submission PR 520*, 21 December 2007.

150 Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

151 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

> [T]he recognition of an EDR scheme already approved under another statutory basis, such as schemes approved by ASIC under the *Corporations Act*, would be a very different role to the Office establishing its own separate benchmarks and an overall EDR scheme approval process. The establishment of such an approval process would have significant resource implications for the Office and is not in the Office's view an appropriate role for it to adopt.[152]

59.129 ARCA stated that, while it agreed in principle with the ALRC's proposal, it should go further, so that membership of an EDR scheme approved by ASIC is a precondition for participation in the credit reporting system.

> This higher threshold is needed to ensure the integrity of the credit reporting process, including data quality, is maintained. To simply restrict default listing ignores the need to maintain the data quality of the other elements of data—which constitute the majority of content for the majority of consumers.[153]

59.130 National Legal Aid agreed with ARCA that the regulations should 'require all entities having access to credit reporting' to be members of an EDR scheme that complies with ASIC standards.[154] Legal Aid Queensland stated that the regulations should provide minimum requirements for both internal dispute resolution and EDR, and suggested that standards for EDR should be modelled on the ASIC policy. Further,

> Where the credit provider is not currently a member of an EDR scheme because they are not utilities or do not provide a financial service as defined under the *Australian Securities and Investment Commission Act 2001* … the credit provider should either join a current financial services scheme or the scheme must meet those minimum standards and be approved by the OPC.[155]

59.131 Stakeholders emphasised that the EDR process should have the power to resolve all aspects of the dispute, not just those involving privacy.[156] Legal Aid Queensland stated that, in its experience, it is often the liability for the debt that is in issue rather than the credit reporting process. It noted that EDR schemes in the financial services sector 'resolve the issue of liability for credit products even though these products are not financial services for the purposes of the ASIC Act'.[157]

59.132 The AFC opposed the ALRC's proposal. It stated that, as a matter of principle, membership of EDR schemes should be voluntary—because 'the evolution of such schemes in the credit area has generally been in the context of self-regulation and voluntary'. Where mandated, such schemes

---

152 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

153 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

154 National Legal Aid, *Submission PR 521*, 21 December 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 19.

155 Legal Aid Queensland, *Submission PR 489*, 19 December 2007, referring to Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999.

156 National Legal Aid, *Submission PR 521*, 21 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

157 Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

> have usually been for financial products which government has itself mandated (eg occupational superannuation) and/or where the business holds the customers' money on promise for a future service (eg insurance).[158]

59.133 In the context of credit reporting, the AFC also considered that

> the cost of such membership for the smaller subscribers to the credit reporting agencies will act as a deterrent to reporting defaults to the overall detriment of the credit reporting system.[159]

ALRC's view

59.134 EDR schemes are already a significant feature of credit reporting complaint handling. In particular, many credit providers are members of the BFSO and TIO schemes and Veda Advantage is a member of the BFSO. Industry and consumer groups generally agreed that the use of EDR in the handling of credit reporting complaints should be facilitated.

59.135 In Chapter 49, the ALRC makes recommendations intended to promote the use of EDR schemes in privacy complaint-handling generally. These include a recommendation to amend the *Privacy Act* to empower the Privacy Commissioner to decline to investigate a complaint where the:

- complaint is being handled by an EDR scheme recognised by the Privacy Commissioner; or
- Privacy Commissioner considers that the complaint would be handled more suitably by an EDR scheme recognised by the Privacy Commissioner, and should be referred to that scheme.[160]

59.136 In the resolution of credit reporting complaints, it is appropriate that EDR schemes provide the first line of dispute resolution beyond the credit provider or credit reporting agency. Such schemes are funded by industry and have expertise in the commercial environment in which their members operate. The ALRC is concerned also to improve OPC conciliation and determination processes and to address the capacity of the OPC to identify and address systemic issues. Placing more of the frontline complaint-handling burden on EDR schemes should assist in achieving these aims.

59.137 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide that credit providers only may list overdue payment information where the credit provider is a member of an EDR scheme approved by the OPC.[161] The main issues raised by stakeholders in response to this proposal concerned:

---

158 Australian Finance Conference, *Submission PR 398*, 7 December 2007.
159 Ibid.
160 Rec 49–2.
161 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–6.

- what role the OPC should have in approving EDR schemes for the purpose of credit reporting complaint handling; and

- whether membership of an approved EDR scheme should be a condition of participation in the credit reporting system.

59.138 As discussed above, some stakeholders have suggested that it would be preferable for EDR schemes to be approved by ASIC, rather than by the OPC.[162] The reasons for this view included that many credit providers are already members of ASIC-approved EDR schemes;[163] and that such schemes are well equipped to deal with aspects of disputes that are unrelated to privacy or the regulation of credit reporting.

59.139 ASIC's EDR approval policy is stated to apply to 'any external complaints resolution scheme operating in the financial system that requires or seeks our approval'. The responsibility of ASIC to approve EDR schemes is part of its role as a financial services regulator, and derives from a number of sources, including the licensing of industry participants and approval of industry codes of practice.[164] As noted above, many credit providers are financial services providers and required by the *Corporations Act* to belong to an EDR scheme approved by ASIC.[165] Some credit providers, for *Privacy Act* purposes are, however, providers of goods and services on credit and are only involved tangentially with the broader financial system. Such organisations are less likely to be members of ASIC-approved EDR schemes.

59.140 As the privacy regulator, it is appropriate that the Privacy Commissioner have oversight of the adequacy of EDR schemes that handle credit reporting complaints. As discussed in Chapter 49 (in relation to the power of the Privacy Commissioner to decline to investigate a complaint), the use by the ALRC of the term 'approved' was not intended to indicate that the OPC would need to establish its 'own separate benchmarks and an overall EDR scheme approval process'.[166] To make this clear, the recommendation should refer to Privacy Commissioner 'recognition', rather than approval, of EDR schemes.

59.141 In the context of credit reporting complaints, the Privacy Commissioner can be expected to recognise EDR schemes already approved by ASIC under the *Corporations Act* and those with another statutory basis, such as the TIO.[167] More broadly, the Privacy Commissioner could recognise schemes that are certified by an

---

162 GE Money Australia, *Submission PR 537*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

163 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

164 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999, [RG 139.14].

165 *Corporations Act 2001* (Cth) s 912A(2)(b).

166 As stated by the OPC: Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

167 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).

independent third party as complying with the ASIC standards[168] and other similar instruments.

59.142 Some stakeholders suggested that membership of an EDR scheme should be a precondition to any participation in the credit reporting system, rather than to only the listing of overdue payment information.

59.143 The ALRC does not agree with this alternative approach. Dispute resolution is needed most in relation to credit reporting information that is adverse to, and may have serious consequences for, the individuals concerned. Membership of an EDR scheme can be expensive. The compliance burden may not justify imposing EDR obligations on credit providers who may, for example, wish to obtain credit reporting information in order to help decide whether to provide goods or services on credit, but do not list defaults.[169]

59.144 The ALRC recommends that the new regulations should provide that credit providers may only list overdue payment or repayment performance history where the credit provider is a member of an EDR scheme recognised by the Privacy Commissioner. As described in Recommendation 55–2, repayment performance history means information indicating whether, over the prior two years, an individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not the number of repayment cycles the individual was in arrears. While repayment performance history will often be 'positive' in terms of the perceived credit worthiness of the individual concerned, where payments are late it is similar to overdue payment information—that is, default listings under current s 18E(1)(b)(vi) of the *Privacy Act.*

Recommendation 59–7 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit providers only may list overdue payment or repayment performance history where the credit provider is a member of an external dispute resolution scheme recognised by the Privacy Commissioner.

Time limits on disputed credit reporting information

59.145 In DP 72, the ALRC noted that individuals effectively have the burden of showing that a disputed debt is listed improperly because the listing will remain part of their credit reporting information until this is shown.[170]

168 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999.

169 The separate issue of reciprocity of data sharing between credit providers is considered in Ch 54.

170 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [55.99].

59.146 This position was considered to be unfair given the relative positions of credit providers and individual consumers who may, for example, never have received a utilities bill.[171] Any delay in resolving a dispute between a credit provider and an individual about the correctness of credit reporting information, including due to the inaction of the credit provider, may prejudice the individual.

59.147 To address this issue, time limits could be placed on certain steps in the dispute resolution process. A model for such a reform is contained in United States credit reporting legislation. In the United States, the FCRA provides that if the completeness or accuracy of information is disputed by a consumer, the credit reporting agency must conduct an investigation and, if the information is not verified, it must be deleted within 30 days.[172]

Discussion Paper proposal

59.148 In DP 72, the ALRC proposed that the new *Privacy (Credit Reporting Information) Regulations* provide that credit providers have an obligation to provide evidence to individuals and dispute resolution bodies to substantiate disputed credit reporting information, such as default listings. If the information is not provided within 30 days the credit reporting agency must delete the information on the request of the individual concerned.[173]

Submissions and consultations

59.149 All stakeholders who addressed the issue were in favour of requiring credit reporting agencies and credit providers to verify the accuracy of disputed credit reporting information within a certain time period.[174]

---

171 See Energy and Water Ombudsman NSW, *Submission PR 225*, 9 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221*, 8 March 2007.

172 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US) s 1681i.

173 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 55–7.

174 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007; Queensland Law Society, *Submission PR 286*, 20 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263*, 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255*, 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 16; J Codrington, *Submission PR 81*, 2 January 2007.

59.150 Stakeholders generally supported the ALRC's proposal, subject to a range of qualifications.[175] The Financial Counsellors Association of Queensland, for example, stated that a 30-day time limit would provide credit providers with 'an incentive to cooperate with consumers and advocates to reach an outcome'.[176]

59.151 Veda Advantage submitted that the new regulations should require that, if a credit provider cannot substantiate disputed credit reporting information within 30 days, then 'the dispute is resolved in the consumer's favour'.[177] ARCA agreed with the proposal but noted that, because it 'reverses the current onus of proof', a strict time limit would

> allow disreputable individuals to engage in 'credit repair' which is currently a significant problem in both the US and the UK. That is, individuals flood credit providers with questions that cannot be answered in the timeframe and thus are rewarded by information being removed from their record.[178]

59.152 ARCA submitted that controls would need to be established to prevent individuals (or third parties on behalf of individuals) from deliberately impeding the dispute resolution process.[179] Similarly, the AFC stated:

> Whatever its actual scale, AFC does not condone credit provider intransigence in the face of bona fide disputed listings. However, if policy is to go in the direction proposed, it must also include practical protections from vexatious and delaying disputation.[180]

59.153 A range of comments were made about the ALRC's proposed time limit and the way in which the time limit is measured. The ANZ stated that a 30 day time limit would be onerous for credit providers, and 60 days would be 'a more realistic timeframe'.[181] Stakeholders suggested that the 30 days commence at the time the individual complaint first is made with the credit provider or credit reporting agency.[182] The Cyberspace Law and Policy Centre also submitted that 'the proposed industry

---

175 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

176 Financial Counsellors Association of Queensland, *Submission PR 371*, 30 November 2007.

177 Veda Advantage, *Submission PR 498*, 20 December 2007.

178 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

179 Ibid. See also GE Money Australia, *Submission PR 537*, 21 December 2007.

180 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

181 ANZ, *Submission PR 467*, 13 December 2007.

182 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

code should address the issue of what happens to the listing during the 30 day challenge period'.[183]

ALRC's view

59.154 Consumer advocates have noted that credit reporting information adverse to an individual's credit worthiness may be in dispute because

- liability for a debt is in dispute (for example, because of mistaken identity or a contractual dispute); or
- the individual had no notice of the obligation and no opportunity to pay (for example, because the credit provider has made billing errors).[184]

59.155 There should be a positive obligation on a credit provider to verify disputed credit reporting information. The ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should provide that, within 30 days, evidence to substantiate disputed credit reporting information must be provided to the individual, or the matter referred to an EDR scheme recognised by the OPC.

59.156 If these requirements are not met, the credit reporting agency should delete or correct the information on the request of the individual concerned. This will provide an incentive for appropriate record-keeping practices and speedy dispute resolution by credit providers and credit reporting agencies. Where information is documented adequately by the credit provider, but remains disputed by the individual, the complaint should be referred to an EDR scheme for resolution.

59.157 There is a range of matters that need to be considered in drafting this provision of the regulations. These include means to deal with frivolous or vexatious complaints and the availability to other credit providers of disputed credit reporting information within the 30 day period.

Recommendation 59–8 The new *Privacy (Credit Reporting Information) Regulations* should provide that, within 30 days, evidence to substantiate disputed credit reporting information must be provided to the individual, or the matter referred to an external dispute resolution scheme recognised by the Privacy Commissioner. If these requirements are not met, the credit reporting agency must delete or correct the information on the request of the individual concerned.

---

183 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007. See also Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

184 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 106.

Investigation and resolution of credit reporting complaints

59.158 Concerns about the existing regulation of credit reporting have focused as much on how the complaints and enforcement provisions have operated in practice as on the substantive obligations. More effective complaint handling and enforcement is seen by many stakeholders as central to making a significant improvement to the existing regulatory framework. Lack of access to effective complaint-handling mechanisms can have serious consequences for individuals who may have no access to credit while, for example, a disputed default listing remains part of their credit reporting information.

59.159 Stakeholders continued to express concern about the role of the OPC in handling credit reporting complaints. The Cyberspace Law and Policy Centre, for example, stated that the efficacy of the ALRC's reforms will depend, in part, on improvements in the complaint-handling policies and procedures of the OPC.[185]

59.160 In Galexia's view, problems stem from the fact that consumer caseworkers have lost confidence in the OPC as regulator and complaint-handling body for credit reporting.

> Overall, we believe there is a real risk that in three to five years time consumers will still be unhappy with the complaints process unless there is a significant change in the approach of the OPC. The other ALRC proposals and enhancements are all worthwhile, but the OPC remains at the centre of credit reporting complaints management and simply must take a more flexible, proactive role and assist in removing technical and bureaucratic obstacles to effective dispute resolution.[186]

59.161 Galexia stated that consumer confidence in the OPC might be enhanced by: ensuring that systemic problems have consequences in terms of credit provider access to credit reporting information; allowing and encouraging the OPC to accept a complaint before it is referred to the respondent; and limiting the OPC's discretion not to investigate a complaint.[187]

59.162 In this context, the reforms recommended in this chapter should be read in conjunction with those in Chapter 49, which deals with the investigation and resolution of privacy complaints generally. In Chapter 49, the ALRC makes a range of recommendations intended to streamline, and increase the transparency of, the resolution of privacy complaints, including in relation to credit reporting complaints. These recommendations are intended, among other things, to:

- free up the Privacy Commissioner from dealing with individual complaints to enable more of a focus on systemic issues;

---

185 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
186 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.
187 Ibid.

- give the Commissioner more discretion not to investigate complaints, including where an EDR mechanism could handle the complaint;

- clarify the Commissioner's conciliation function in the *Privacy Act* and give complainants and respondents the power to compel a determination when conciliation has failed; and

- give the Commissioner power to remedy systemic issues, for example, by requiring an organisation, such as a credit reporting agency, to undertake prescribed action for the purpose of ensuring compliance with the model UPPs.

Penalties

59.163 Part IIIA of the *Privacy Act* creates a range of credit reporting offences. These include, for example, offences relating to:

- credit providers using or disclosing personal information contained in credit reports other than as permitted;[188]

- credit reporting agencies or credit providers intentionally giving out a credit report that contains false or misleading information;[189]

- persons intentionally obtaining unauthorised access to credit information files or credit reports;[190] and

- persons obtaining access to credit information files or credit reports by false pretences.[191]

59.164 In response to IP 32, stakeholders expressed a range of views about penalties. Some stakeholders considered that the existing penalties are sufficiently broad or opposed any new penalty provisions.[192] Other stakeholders favoured the introduction of new civil or administrative penalties.[193]

Discussion Paper proposals

59.165 In DP 72, the ALRC proposed that the *Privacy Act* be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy

---

188 *Privacy Act 1988* (Cth) ss 18L(2), 18N(2).
189 Ibid s 18R(2).
190 Ibid s 18S(3).
191 Ibid s 18T.
192 Optus, *Submission PR 258*, 16 March 2007; National Credit Union Association Inc, *Submission PR 226*, 9 March 2007.
193 Queensland Law Society, *Submission PR 286*, 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277*, 3 April 2007; Australian Privacy Foundation, *Submission PR 275*, 2 April 2007; Consumer Action Law Centre, *Submission PR 274*, 2 April 2007.

of an individual. The ALRC also proposed that the OPC develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty is made.[194]

59.166 Finally, the ALRC proposed that the *Privacy Act* should be amended to remove the credit reporting offences and allow a civil penalty to be imposed where there is a serious or repeated breach of the regulations.[195]

Submissions and consultations

59.167 Stakeholders supported the ALRC's proposal to repeal the credit reporting offences and replace them with a civil penalties regime.[196]

59.168 ARCA submitted that, in addition to the proposed civil penalties, severe or repeated breach of the new regulations should result in temporary or permanent suspension or exclusion from the credit reporting system, in accordance with processes set out in a code of conduct.[197] Galexia stated that

> it may be useful for the industry to have a self-policing role in addition to the sanctions available in the Regulations. For example, the ability to limit access to credit reporting information where organisations are found to have engaged in a systemic breach might also apply to systemic breaches of the potential industry Code. Sanctions could be applied by a Code compliance body, and might include suspension or restricted access to credit reporting information, or requirements for specific performance such as corrective advertising, training, changes to procedures etc.[198]

59.169 The OPC suggested that, in addition to the civil penalty regime, the *Privacy Act* should specify particular conduct that is considered to be a 'serious' breach of credit reporting provisions, based on the existing credit reporting offences under Part IIIA of the Act.[199]

ALRC's view

59.170 In Chapter 50, the ALRC recommends that the *Privacy Act* should be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual.[200] Part IIIA creates a wide range of credit reporting

---

194 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 46–2.

195 Ibid, Proposal 55–8.

196 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 401*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

197 Australasian Retail Credit Association, *Submission PR 352*, 29 November 2007.

198 Galexia Pty Ltd, *Submission PR 465*, 13 December 2007.

199 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

200 Rec 50–2.

offences. These offences are unnecessary, in light of the recommended civil penalties regime, and should not be retained.

59.171 The ALRC understands that no prosecutions have ever been launched under the credit reporting offence provisions. At least some of the relevant conduct is covered, in any case, by other offences under Commonwealth legislation. The *Criminal Code*, for example, creates an offence in respect to unauthorised access to, or modification of, data held in a computer to which access is restricted.[201]

59.172 Since the enactment of the credit reporting provisions, civil penalty regimes have become a more common means to enforce consumer protection laws including, for example, under the financial services civil penalty provisions of the *Corporations Act*[202] and the uniform *Consumer Credit Code*.[203] The ALRC considers that a civil penalty regime is a more appropriate enforcement mechanism for breaches of credit reporting regulation than the suite of criminal offences currently provided for in the Act.

59.173 In Chapter 54, the ALRC recommends that credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the OPC, develop a credit reporting code.[204] It may be desirable for this code to provide for penalties, imposed by contract, for breach of the regulations or the code itself. Sanctions for non-compliance, such as suspension or expulsion from the credit reporting system, may raise competition issues and require authorisation by the Australian Competition and Consumer Commission.

Recommendation 59–9 The *Privacy Act* should be amended to remove the credit reporting offences and allow a civil penalty to be imposed as provided for by Recommendation 50–2.

201 *Criminal Code Act 1995* (Cth) s 478.1.
202 *Corporations Act 2001* (Cth) ss 1317DA, 1317E(1)(ja)–(jg).
203 *Consumer Credit Code* pt 6. The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories.
204 Rec 54–9.

Part H

Health Services and Research

60. Regulatory Framework for Health Information

Contents

Introduction

60.1 In 2004, the Australian Government Department of Health and Ageing (DOHA) stated that:

> Privacy is a fundamental principle underpinning quality health care. Without an assurance that personal health information will remain private, people may not seek the health care they need which may in turn increase the risks to their own health and the health of others. Indeed consumers regard health information as different to other types of information and consider it to be deeply personal.[1]

60.2 The personal health information of health consumers was traditionally protected by the ethical and legal duties of confidentiality. These duties are owed by health service providers—such as doctors, dentists, nurses, physiotherapists and pharmacists—to health consumers and prevent the use of personal health information for a purpose that is inconsistent with the purpose for which the information was provided. A legal duty of confidentiality may arise in equity, at common law, or under contract. In addition, health service providers are often subject to confidentiality provisions in professional codes of conduct[2] and, if they are employed in the public sector, may be subject to legislative secrecy provisions.

---

1 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

2 See, eg, Australian Medical Association, *Code of Ethics* (2004), s 1.1(l). Confidentiality is also discussed in Chs 8, 15 and 16.

60.3 Duties of confidentiality recognise the dignity and autonomy of the individual,[3] as well as the public interest in fostering a relationship of trust between health service providers and health consumers to ensure both individual and public health outcomes.[4] Such duties are not absolute and there are circumstances in which the law permits, and sometimes requires, the disclosure of confidential personal health information.[5]

60.4 Where legislation establishes health agencies or provides the basis for health-related functions to be carried out, officers of those agencies and others performing functions under the legislation frequently are subject to secrecy provisions that prohibit them from disclosing personal information about third parties except in the course of their duties.[6] There is also a range of disease-specific legislation that may include provisions intended to protect individuals' health information. For example, legislation dealing with HIV/AIDS generally requires the use of codes to link test results with individuals rather than including personal details on test request forms.[7]

60.5 More recently, privacy legislation has been introduced in a number of Australian jurisdictions specifically to regulate the handling of personal health information.[8] An overview of privacy regulation in the states and territories, including health privacy regulation, is provided in Chapter 2. Health service providers continue to be subject to secrecy provisions and duties of confidentiality. Although the regimes exist side by side, Marilyn McMahon has suggested that:

> In practice the less costly, more 'user friendly' complaint procedures offered under the privacy regimes may in fact mean that they increasingly 'cover the field' and that the traditional, common law remedies for protecting confidentiality become archaic.[9]

60.6 In its submission to ALRC Issues Paper 31, *Review of Privacy* (IP 31),[10] DOHA noted the following changes to health service delivery that may have implications for the way that health information is handled:

> There is an increasing focus on coordinated multi-team care through a mix of public and private providers. In delivering healthcare services in this environment, a large

---

3 M McMahon, 'Re-thinking Confidentiality' in I Freckelton and K Petersen (eds), *Disputes & Dilemmas in Health Law* (2006) 563, 579.

4 P Finn, 'Confidentiality and the "Public Interest"' (1984) 58 *Australian Law Journal* 497, 502.

5 See, eg, *Public Health Act 1991* (NSW) s 14; *Health Act 1958* (Vic) s 138 in relation to notifiable diseases. See also the discussion of professional confidential relationship privilege in Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [15.3]–[15.14], [15.31]–[15.44].

6 See, eg, *National Health Act 1953* (Cth) s 135A; *Health Insurance Act 1973* (Cth) s 130; *Health Administration Act 1982* (NSW) s 22; *Health Services Act 1988* (Vic) s 141.

7 R Magnusson, 'Australian HIV/AIDS Legislation: A Review for Doctors' (1996) 26 *Australian & New Zealand Journal of Medicine* 396.

8 *Privacy Act 1988* (Cth); *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Personal Information Protection Act 2004* (Tas); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act 2002* (NT).

9 M McMahon, 'Re-thinking Confidentiality' in I Freckelton and K Petersen (eds), *Disputes & Dilemmas in Health Law* (2006) 563, 583.

10 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).

> volume of information about individuals moves frequently between the public and private sectors, and across State and Territory boundaries. To provide an indication of the volume and frequency of these communications, there were 4.2 million in-patient discharges from public hospitals in 2003/04, with about one-half of these being on the 'same-day'. A number of information exchanges between providers in the public and private sectors may have been associated with each of these discharges, including for referral, discharge or enquiry with a patient's GP, and with contracted pathology or radiology diagnostic services.[11]

60.7 Technology is developing to help deal with these challenges. DOHA went on to note that:

> Australia is on the threshold of major developments in national e-health systems and the use of telehealth services. The aim of these systems is to enable health information to be shared more reliably, securely and efficiently between healthcare providers with the aim of delivering safe care and better health outcomes for individuals. The use of these systems will increase the volume and frequency of communications and may mean the individual whom the information concerns is located in a different State or Territory to the holder of the information. New work systems and practices will emerge as e-health systems are developed and implemented, and the use of telehealth services expand.[12]

60.8 In this and the following chapters, the ALRC considers how to meet these challenges, while ensuring that individuals' health information is handled appropriately. In Chapter 61, the ALRC examines developments in electronic health records systems. This chapter considers the need for greater national consistency in health privacy regulation. This issue is closely related to the discussion of national consistency in privacy regulation more generally in Chapter 3.

National consistency

Issues and problems

Overlapping and inconsistent legislation

60.9 Chapter 2 provides an overview of privacy regulation in Australia. The position is particularly complex in the area of health information for a number of reasons. In general terms, the *Privacy Act* regulates the handling of health information in the Australian Government and ACT public sectors and in the private sector. A number of the states and territories have passed legislation that regulates the handling of health information in the state or territory public sector and the private sector.[13] The following

---

11 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

12 Ibid.

13 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Personal Information Protection Act 2004* (Tas); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act 2002* (NT). Other state and territory legislation may also have an impact on the handling of health information, for example, the New South Wales Government Department of Health, *NSW Health Privacy Manual (Version 2)* (2005) includes information on the *Health Administration Act 1982*

table provides an overview of the jurisdictional scope of some of the major pieces of health privacy legislation in Australia.

Table 60–1: Privacy Legislation Regulating the Handling of Health Information		
Jurisdiction	**Public Sector**	**Private Sector**
Commonwealth	*Privacy Act 1988* (Cth)	*Privacy Act 1988* (Cth)
New South Wales	*Health Records and Information Privacy Act 2002* (NSW)	*Health Records and Information Privacy Act 2002* (NSW) *Privacy Act 1988* (Cth)
Victoria	*Health Records Act 2001* (Vic)	*Health Records Act 2001* (Vic) *Privacy Act 1988* (Cth)
Queensland	[See 60.10 below]	*Privacy Act 1988* (Cth)
Western Australia	[See 60.12 below]	*Privacy Act 1988* (Cth) [See also 60.12 below]
South Australia	[See 60.11 below]	*Privacy Act 1988* (Cth)
Tasmania	*Personal Information Protection Act 2004* (Tas)	*Privacy Act 1988* (Cth)
ACT	*Health Records (Privacy and Access) Act 1997* (ACT) *Privacy Act 1988* (Cth)	*Health Records (Privacy and Access) Act 1997* (ACT) *Privacy Act 1988* (Cth)
Northern Territory	*Information Act 2002* (NT)	*Privacy Act 1988* (Cth)

(NSW); *Mental Health Act 1990* (NSW); *Public Health Act 1991* (NSW); *State Records Act 1989* (NSW); and the *Freedom of Information Act 1989* (NSW).

60.10 Although there is no specific privacy legislation regulating the handling of health information in the public sector in Queensland, Western Australia or South Australia, such information may be protected in other ways. In Queensland, the state government has introduced a privacy policy by administrative, rather than legislative, means. *Information Standard 42 on Information Privacy*[14] is based on the Information Privacy Principles (IPPs) and *Information Standard 42A on Information Privacy for the Queensland Department of Health*[15] is based on the National Privacy Principles (NPPs). Both standards are issued under the *Financial Management Standard 1997* (Qld).

60.11 The South Australian Government also has introduced a privacy policy by administrative, rather than legislative, means. The *PC012—Information Privacy Principles Instruction* is based on the IPPs. The Department of Health *Code of Fair Information Practice* is based on the NPPs.

60.12 In Western Australia, no legislation or formal administrative arrangements are currently in place. The Information Privacy Bill 2007, however, was introduced into the Western Australian Parliament on 28 March 2007. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information in the public and private sectors.[16] It contains a set of eight Information Privacy Principles and 10 Health Privacy Principles.

60.13 As indicated in Table 60–1 above, both the federal *Privacy Act* and state or territory legislation regulate the handling of health information in the private sector in a number of jurisdictions. The New South Wales *Health Records and Information Privacy Act* and the Victorian *Health Records Act* contain a set of Health Privacy Principles (HPPs). The ACT *Health Records (Privacy and Access) Act* contains a set of Privacy Principles. Private sector health service providers in these jurisdictions are therefore required to comply with two sets of principles: the NPPs in the *Privacy Act* and the relevant set of HPPs or Privacy Principles. While the HPPs in New South Wales and Victoria are based on the NPPs, they are not identical, and in some cases impose different standards. The ACT Privacy Principles are based on the IPPs, but have been modified to apply specifically to health information.[17]

---

14 Queensland Government, *Information Standard 42—Information Privacy* (2001).

15 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001).

16 A related Bill, the Freedom of Information Amendment Bill 2007 (WA), was introduced on the same day. This Bill provides the Privacy and Information Commissioner with powers to resolve FOI complaints by conciliation. At the time of writing in April 2008, both Bills were awaiting passage by the Legislative Council.

17 Explanatory Memorandum, Health Records (Privacy and Access) Bill 1997 (ACT).

60.14 In addition, the scope of the state and territory legislation may differ from the federal legislation. For example, the Victorian *Health Records Act* covers small business operators and employee records—unlike the *Privacy Act*.

60.15 The New South Wales and Victorian HPPs and the ACT Privacy Principles also differ from each other, so that information passing from one jurisdiction to the other may become subject to a different set of rules. This causes particular difficulty for health service providers and researchers operating across jurisdictional borders or nationally.

The public-private sector divide

60.16 Another problem arises in jurisdictions like Tasmania, where health information in the public sector is regulated by the *Personal Information Protection Act*, while health information in the private sector is regulated by the *Privacy Act.* The *Personal Information Protection Act* contains a set of Personal Information Protection Principles (PIPPs) that are not identical to the NPPs.

60.17 In the health services context, individuals regularly move between public and private sector health service providers. For example, an individual may be referred by a private sector general practice for treatment in a public hospital. In some situations the public and private sector providers work side by side, for example, where an individual is treated as a private patient in a public hospital. This means that health information may be subject to two different sets of privacy principles at the same time.

60.18 Similar problems arise because of the distinction in the *Privacy Act* between public sector agencies and private sector organisations. Agencies are bound by the IPPs; organisations are bound by the NPPs. There are also circumstances in which an organisation or agency may be subject to both the IPPs and the NPPs. For example, an Australian Government contractor may be bound to comply with the NPPs as an organisation, while at the same time being bound by contract to comply with the IPPs in relation to information held pursuant to that contract.[18] These issues, including the need for a single set of principles in the *Privacy Act*, are considered in detail in Parts C and D of this Report.

The OPC Review

60.19 The review by the Office of the Privacy Commissioner of the private sector provisions of the *Privacy Act 1988* (Cth) (the OPC Review) identified the following problems that arise because of inconsistency and overlap in the regulation of personal information:

---

18 See *Privacy Act 1988* (Cth) s 95B in relation to requirements for Commonwealth contracts; and s 6A(2)—no breach of an NPP if an act or practice of the contracted service provider is authorised by a provision of the contract that is inconsistent with the NPP.

- increased compliance costs, particularly where businesses are conducted across jurisdictional boundaries;
- confusion about which regime regulates particular businesses;
- forum shopping to exploit differences in regulation; and
- uncertainty among consumers about their rights.[19]

60.20 In its submission to the OPC Review, DOHA stated that:

> The co-existence of Commonwealth, state and territory health information privacy legislation has created a significant burden on private sector health care services in understanding and meeting respective obligations, as well as confusion for health consumers affected by dual legislative instruments.[20]

60.21 In relation to health and medical research, the National Health and Medical Research Council (NHMRC) stated in its submission to the OPC Review that:

> There is evidence that legitimate and ethical activities (which in some cases are vital to the quality provision of health care or the conduct of important health and medical research) are being delayed or proscribed because some key decision-making bodies are unable to determine, with sufficient confidence, whether specific collections, uses and/or disclosures of information accord with legislative requirements. The adoption of a highly conservative approach is resulting in excessive administrative effort and a reluctance to approve the legitimate use and disclosure of health information for the purposes of health care, as well as health and medical research.[21]

60.22 Those making submissions to the OPC Review overwhelmingly expressed the view that the existing state of health privacy law in Australia was unsatisfactory for health service providers, health and medical researchers and individuals.[22] In addition, concern was expressed that the problem would get worse as electronic health records become commonplace.[23]

60.23 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the NHMRC recommended that:

---

19 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 66–68. The costs of legislative inconsistency and regulatory fragmentation are considered in detail in Ch 14.

20 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

21 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

22 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

23 Ibid, 43.

> As a matter of high priority, the Commonwealth, States and Territories should pursue the harmonisation of information and health privacy legislation as it relates to human genetic information. This would be achieved most effectively by developing nationally consistent rules for handling all health information.[24]

A recommended solution

60.24 As discussed in Chapter 3, the *Privacy Act* expressly allows state and territory privacy legislation to operate to the extent that it is capable of operating concurrently with the *Privacy Act*. Section 3 of the *Privacy Act* indicates the Australian Parliament's intention that the Act should not 'cover the field' in the constitutional sense and that state and territory legislation should be allowed to operate alongside the *Privacy Act*, to the extent that such laws are not directly inconsistent with the *Privacy Act*. Where state and territory law is directly inconsistent with the *Privacy Act*—that is, it is not capable of operating concurrently with the Act—that law will be invalid to the extent of the inconsistency.[25]

Discussion Paper proposals

60.25 In DP 72, the ALRC made a number of proposals aimed at achieving greater national consistency in the regulation of personal information, including health information. These included the consolidation of the IPPs and the NPPs into a single set of Unified Privacy Principles (UPPs) to apply across the public and private sectors.[26]

60.26 The ALRC also proposed that the *Privacy Act* be amended to make clear that the Act was intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations in the private sector. In particular, the following state and territory laws were to be excluded from applying in the private sector: the *Health Records and Information Privacy Act 2002* (NSW); the *Health Records Act 2001* (Vic); the *Health Records (Privacy and Access) Act 1997* (ACT); and any other laws prescribed in the regulations.[27] In addition, the ALRC proposed that the states and territories enact legislation regulating the handling of personal information in each state or territory's public sector and that this legislation apply the UPPs and amending regulations as in force under the *Privacy Act* from time to time.[28] This was intended to ensure that the same UPPs, as well as proposed regulations dealing specifically with health information, would apply in every jurisdiction and across the public sector and the private sector.[29]

---

24 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–1.

25 Section 109 of the *Australian Constitution* provides that 'When a law of a State is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid'.

26 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 15–2.

27 Ibid, Proposal 4–1.

28 Ibid, Proposal 4–4.

29 The recommended *Privacy (Health Information) Regulations* are discussed in Ch 63.

Submissions and consultations

60.27 There was strong support in submissions and consultations for greater national consistency in the regulation of health information.[30] The NHMRC expressed the view that:

> the current state of privacy regulation in Australia is entirely unsatisfactory. Its complexity is impacting on the proper provision of health care and the conduct of important health and medical research, in addition to creating significant unnecessary compliance costs.
>
> The NHMRC considers that a solution to the current problem of an unnecessarily complex privacy regulatory regime needs to be identified and implemented as a priority.
>
> The NHMRC supports the development of a national set of privacy principles that apply to all health information uniformly across the public and private sectors.[31]

60.28 The Pharmacy Guild of Australia noted that the 'marginally different laws on the handling of health information' across Australia had caused problems for the national initiative 'Project STOP', making implementation of the project complex and time consuming. Project STOP is a program to track pseudoephedrine sales by requiring pharmacists to record personal information about any person requesting pseudoephedrine-based products in a web-based database.[32]

60.29 A number of insurance bodies discussed the difficulties that overlapping and inconsistent health privacy legislation posed for their national operations.[33] Other stakeholders expressed concern about the difficulty of conducting research or providing health services across jurisdictional boundaries. It was noted that health consumers often shift between jurisdictions and should receive the same level of protection in every state and territory.[34] The New South Wales Guardianship Tribunal noted that the inconsistencies and complexities in privacy law caused particular problems for those working in the disability sector, as people with disabilities often receive services from a range of public and private organisations.[35]

---

30 See, for example, Unisys, *Submission PR 569*, 12 February 2008; Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; Royal Women's Hospital Melbourne, *Submission PR 108*, 15 January 2007.

31 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

32 Pharmacy Guild of Australia, *Submission PR 433*, 10 December 2007.

33 AAMI, *Submission PR 147*, 29 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007.

34 Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; A Smith, *Submission PR 79*, 2 January 2007; R Magnusson, *Submission PR 3*, 9 March 2006.

35 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007.

60.30 The OPC expressed the view that:

> there is a strong need to clarify the application of the *Privacy Act* to private sector health service providers. Section 3 of the *Privacy Act* should be amended to make clear that the National Privacy Principles 'cover the field' for the regulation of private sector health service providers. This would address a key source of uncertainty and potential fragmentation in health privacy regulation in Australia.[36]

60.31 A number of stakeholders expressed support for a cooperative approach to achieving national consistency, rather than amending s 3 of the *Privacy Act* to exclude state and territory legislation.[37] The Government of South Australia did not support the Australian Government legislating to 'cover the field', expressing concern about the possibility that the *Privacy Act* might have an adverse impact on the operation of state legislation dealing with issues such as compulsory notification in relation to child abuse and notifiable diseases.[38] The Western Australian Department of Health noted that the regulation of health privacy has important implications for areas of state responsibility including the delivery of health care and the management of health services. The Department was of the view that health privacy should be regulated at the state level.[39]

60.32 The Office of the Health Services Commissioner (Victoria) suggested that state health privacy legislation was important to allow health consumers access to local complaint-handling bodies:

> As well as administering the *Health Records Act*, HSC [the Office of the Health Services Commissioner] also handles complaints about health services in Victoria. HSC is therefore familiar with the workings of the local health system. This is very important when handling complaints about possible breaches of health privacy. HSC receives a number of complaints where the person is complaining about the health service they received as well as a breach of health privacy. Both complaints are dealt with together, as there is often an overlap of issues.[40]

ALRC's view

60.33 The importance of national consistency in the handling of personal information is examined in detail in Chapter 3. Although the health information privacy legislation in New South Wales, Victoria and the ACT highlights the problems caused by overlapping and inconsistent legislation, the issue is not confined to the handling of health information. The ALRC's main proposals in relation to national consistency are framed in relation to personal information (including health information), and can be found in Chapter 3.

---

36 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

37 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006.

38 Government of South Australia, *Submission PR 187*, 12 February 2007.

39 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

40 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

60.34 The ALRC has found that inconsistency and fragmentation in privacy regulation causes a number of problems, including unjustified compliance burden and cost, and impediments to information sharing and national initiatives in the provision of health services and the conduct of research.[41] The ALRC has concluded that national consistency should be one of the goals of privacy regulation in Australia and that personal information should attract similar protection, whether that personal information is being handled by an Australian Government agency, a state or territory government agency or a private sector organisation.

60.35 In Chapter 3, the ALRC recommends that the *Privacy Act* be amended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information in the private sector.[42] In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations: the *Health Records and Information Privacy Act 2002* (NSW); the *Health Records Act 2001* (Vic); and the *Health Records (Privacy and Access) Act 1997* (ACT).

60.36 Other state and territory laws may be introduced to regulate the handling of personal information or health information in the private sector, for example, the Information Privacy Bill 2007 (WA). The ALRC therefore recommends that the *Privacy Act* be amended to allow the making of regulations to exclude such laws, if necessary, in the future.[43]

60.37 The ALRC notes state and territory concerns about the interaction of the amended *Privacy Act* with state and territory laws. These laws include, for example, state and territory public health Acts requiring health service providers to collect and record certain information about health consumers with notifiable diseases, such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[44] Other state and territory laws contain provisions that require mandatory reporting when a child is suspected of being at risk of harm.[45]

60.38 The model UPPs will allow most of these laws to operate under express exceptions for acts or practices that are 'required or authorised by or under law'.[46] In relation to areas that are not covered adequately by such exceptions, the ALRC recommends that the Australian Government, in consultation with state and territory governments, develop a list of specific 'preserved matters' for the purposes of the

---

41 See Ch 14.
42 Rec 3–1.
43 Rec 3–1.
44 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.
45 See, eg, *Children, Youth and Families Act 2005* (Vic) pt 4.4; *Child Protection Act 1999* (Qld); *Children's Protection Act 1993* (SA) pt 4; *Children Young Persons and Their Families Act 1997* (Tas) pt 3.
46 See, eg, the exception to the 'Use and Disclosure' principle for use and disclosure that is 'required or authorised by or under law'.

Privacy Act.[47] The Act should not apply to the exclusion of a state or territory law so far as the law deals with a 'preserved matter'.

60.39 In relation to the handling of personal information in the state and territory public sectors, the ALRC recommends an intergovernmental agreement. A major cause of inconsistency in Australian privacy laws is that the *Privacy Act* and state and territory privacy laws include similar, but not identical, privacy principles. It is the ALRC's view that the most effective method of dealing with these inconsistencies is the adoption of identical privacy principles across Australia. The intergovernmental agreement would provide that state and territory privacy legislation apply the model UPPs and any relevant regulations made under the *Privacy Act* that modify the application of the UPPs.[48] These would include the new *Privacy (Health Information) Regulations*, discussed further below and in Chapter 63, as in force under the Act from time to time.

60.40 The ALRC does not recommend that the states and territories be required to develop legislation that exactly mirrors the *Privacy Act*. Apart from the specified elements, the states and territories would be free to develop legislation in relation to their public sectors that accommodates existing state and territory information laws and compliance and enforcement mechanisms. The ALRC does recommend, however, that definitions of key terms used in the *Privacy Act* (such as 'personal information', 'sensitive information' and 'health information') should be adopted in state and territory privacy legislation.[49]

Complaint handling

60.41 In DP 72, the ALRC considered the issue of complaint handling under the various federal, state and territory privacy laws. Because of overlapping legislation, complaints against private sector health service providers in Victoria, for example, may be handled by either the OPC or the Victorian Health Services Commissioner. The ALRC's proposal that the *Privacy Act* operate to the exclusion of state and territory health privacy law in the private sector would have removed this jurisdiction from state and territory complaint-handling authorities. The ALRC recognised, however, that there were advantages to handling complaints at a local level. The local complaint handler often has contacts and relationships with local providers, and is in a better location to conduct conciliation conferences.

60.42 In DP 72, the ALRC proposed that the *Privacy Act* be amended to allow the Privacy Commissioner to delegate his or her powers relating to the handling of complaints to state and territory authorities.[50] This proposal was intended to allow the Privacy Commissioner to enter into agreements with state or territory authorities, such

47 Rec 3–3.
48 Rec 3–4.
49 Rec 3–4.
50 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–3.

as the Office of the Victorian Health Services Commissioner, to allow those authorities to handle complaints under the *Privacy Act*. In DP 72, the ALRC also proposed that the Privacy Commissioner consider delegating the power to handle complaints about the handling of health information by private sector health service providers to state and territory health complaint agencies.[51]

Submissions and consultations

60.43 There was a mixed response from stakeholders to this proposal. Some were opposed; some offered qualified support; and others were fully supportive. The OPC did not support the proposal, on the basis that it would introduce a level of complexity and uncertainty into the complaint handling process. If this function were delegated, the OPC expressed the view that it would be necessary to ensure that the state or territory authority had complaint-handling processes and remedies that were consistent with those of the OPC. The OPC noted that proximity to the parties to a complaint was no longer as important as it had been in the past, given modern communication options such as email and voice and video conferencing.[52]

60.44 The Australian Privacy Foundation gave qualified support, stating that it would support the ALRC's proposal only if it incorporated a guarantee that complaint mechanisms and remedies at the state and territory level were of at least the same standard as those provided in the *Privacy Act*.[53]

60.45 In its submission, the Australian Medical Association (AMA) expressed concern about the proposal, noting that the AMA had developed a good working relationship with the OPC and that state and territory health complaint agencies may lack the expertise and training to deal with privacy issues.[54] The Health Informatics Society of Australia expressed a preference for a well resourced, nationally consistent complaint-handling process, rather than a system in which this function was delegated to the states and territories.[55]

60.46 The Government of South Australia did not support the proposal on the basis that, in its view, health information does not need to be treated differently from other types of personal information. The South Australian Government also noted that this proposal would result in increased resourcing and staff development needs for the South Australian Health and Community Services Complaints Commissioner.[56]

---

51 Ibid, Proposal 56–1.
52 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
53 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
54 Australian Medical Association, *Submission PR 524*, 21 December 2007.
55 Health Informatics Society of Australia, *Submission PR 554*, 2 January 2008.
56 Government of South Australia, *Submission PR 565*, 29 January 2008.

60.47 The Victorian Office of the Health Services Commissioner endorsed the importance of handling health privacy complaints locally but did not support the proposal to achieve this through delegation:

> One reason for the effectiveness of state and territory health complaint agencies is their independence and the long standing relationships they have built up within the health sector. HSC is concerned that in acting as a delegate to the Privacy Commissioner, the state and territory agencies may be restricted in the independence of their decision making and their ability to respond to local circumstances. There are also resource implications that need to be taken into account.[57]

60.48 On the other hand, a range of stakeholders expressed support for the ALRC's proposal.[58] The Australian Government Department of Human Services noted that the ALRC's proposed approach would allow complaints to be dealt with as quickly and efficiently as appropriate and possible. The Department, and a number of other stakeholders, noted that there would be a need to ensure some level of consistency in complaint handling on behalf of the OPC, and that the OPC would need to consider the capacity, expertise and level of resources available to state and territory health complaint agencies.[59] Medicare Australia commented that health privacy complaints often arise in the context of a wider complaint about health service provision and that health complaint agencies can deal with all the related issues. Medicare Australia also noted that such agencies are more accessible and have a good understanding of the context in which such issues arise.[60]

60.49 In addition, the NHMRC suggested that it would be necessary to develop clear and transparent criteria on which to base the decision to delegate the complaint-handling function. NHMRC expressed the view that cross-jurisdictional complaints and those with potentially national implications should be investigated by the Privacy Commissioner rather than being delegated to state or territory health complaint agencies.[61]

ALRC's view

60.50 In Chapter 49, the ALRC examines the options for investigating and resolving complaints under the *Privacy Act*, including referral of complaints to registered external dispute resolution schemes and state and territory complaint-handling

---

57 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.

58 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Northern Territory Government Department of Health and Community Services, *Submission PR 480*, 17 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

59 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

60 Medicare Australia, *Submission PR 534*, 21 December 2007.

61 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

authorities. The ALRC concludes that such referral has the potential to increase efficiency in dispute resolution, and to provide parties with a one-stop-shop for complaints that involve both privacy and service delivery issues.

60.51 In that chapter, the ALRC recommends that the *Privacy Act* be amended to enable the Privacy Commissioner to delegate all or any of his or her powers in relation to complaint handling to a state or territory authority.[62] The Commissioner would not be required to delegate his or her powers unless he or she was of the view that such delegation would be appropriate and effective.

60.52 This leaves open the possibility that the Privacy Commissioner could delegate the power to handle complaints relating to health information to a state or territory health complaints authority. Under any such arrangement, the state or territory authority would be able to handle complaints under the *Privacy Act* and to exercise the powers of the Privacy Commissioner. Thus, the broad framework for handling complaints would be consistent with the framework imposed on the OPC complaint-handling process. The Commissioner, however, could include other stipulations in the arrangements surrounding any such delegation.

60.53 The ALRC agrees with stakeholders that it will be necessary for the Privacy Commissioner to consider issues of capacity, expertise, and resources before entering into such an arrangement with a state or territory authority. The ALRC also agrees with the NHMRC that cross-jurisdictional complaints and those with national implications may be more appropriately dealt with at the national level. It may be, for example, that the Privacy Commissioner decides to delegate only the conciliation function to a state and territory authority and to retain the determination-making power at the national level.

60.54 In summary, it would be valuable for the Privacy Commissioner to consider delegating the power to handle complaints under the *Privacy Act* in relation to health information to state and territory health complaint authorities. On the basis of the recommendations in Chapter 49, this will be possible under the amended Act. The ALRC does not consider it necessary, therefore, to make a further recommendation in this chapter.

A separate set of Health Privacy Principles?

60.55 At the federal level, health information is generally treated as a sub-set of 'sensitive information' under the *Privacy Act*, although there are a number of provisions and principles that deal specifically with health information. As noted above, three of the states and territories have taken a different approach. New South

62 Rec 49–3.

Wales, Victoria and the ACT have separate legislation—including a separate set of privacy principles—dealing specifically with health information.[63]

60.56 In considering the Privacy Amendment (Private Sector) Bill 2000 (Cth), the House of Representatives Standing Committee on Legal and Constitutional Affairs noted that the inclusion of health information was the most contentious aspect of the Bill.[64] Some stakeholders expressed the view that health information should not be included in the Bill because:

- the health sector is so different from other sectors that the attempt to incorporate it within the general framework of the Bill was misguided;
- the rights contained in the Bill enabling individuals to obtain access to their own health information were inadequate; and
- the Bill created inconsistent standards governing privacy rights in the public and private sectors.[65]

60.57 Other stakeholders expressed the view that health information should be included in the Bill on the basis that such information is held in a variety of contexts other than the health services context—such as insurance and employment—and that a different approach to the handling of health information would make it difficult to achieve a nationally consistent privacy framework. In addition, stakeholders expressed the view that the modifications made in relation to the handling of sensitive information in the NPPs provided an appropriate and workable framework for the handling of health information.[66]

60.58 The House of Representatives Standing Committee concluded that health information should be included in the Bill.[67] The Committee expressed concern, however, about 'the resulting plethora of principles that will then apply to both the public and private health sectors'.[68] The Committee recommended that:

> the Government encourage all relevant parties to reach an agreed position on the major issues raised in the evidence to this inquiry, such as the harmonisation of privacy principles applicable to the public and private sectors, as a matter of urgency.[69]

---

63 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

64 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [6.2].

65 Ibid, [6.12].

66 Ibid, [6.7]–[6.10].

67 Ibid, rec 15.

68 Ibid, [6.35].

69 Ibid, rec 14.

60.59 The issue of national consistency was central to these recommendations, but the Committee did not consider in any detail the argument that health information and the health context are so unique that they require a separate set of principles.

The Privacy Act 1988 (Cth)

60.60 As discussed in Chapter 5, the federal *Privacy Act* originally regulated the handling of personal information by Australian Government and ACT public sector agencies. The Act required agencies to apply the IPPs in handling all personal information. The IPPs do not draw a distinction between personal information and sensitive information or health information.[70]

60.61 The *Privacy Amendment (Private Sector) Act 2000* (Cth), and the NPPs set out in that Act, however, do draw a distinction between personal information, sensitive information and health information. 'Sensitive information' is defined to include 'health information' and is given a higher level of protection under the NPPs than other personal information. Sensitive information:

- may be collected only with consent, except in specified circumstances;[71]
- must not be used or disclosed without consent for a secondary purpose unless that purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual;[72]
- must not be used for the secondary purpose of direct marketing;[73] and
- cannot be shared by 'related bodies corporate' in the same way that they may share other personal information.[74]

60.62 The NPPs also make special and specific provision for the collection, use and disclosure of health information in some circumstances, for example, for the: management, funding and monitoring of a health service;[75] and for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety.[76]

---

70 The IPPs and NPPs are discussed in detail in Part D of this Report.
71 *Privacy Act 1988* (Cth) sch 3, NPP 10.
72 Ibid sch 3, NPP 2.1(a).
73 Ibid sch 3, NPP 2.1(c).
74 Ibid s 13B.
75 The management, funding and monitoring of health services is discussed in Ch 63.
76 Research is discussed in detail in Chs 64, 65 and 66.

60.63 In addition, NPP 10.2 provides for the collection of health information without consent where the information is necessary to provide a health service to the individual. The information must be collected only as required or authorised by or under law, or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality that bind the organisation.[77]

60.64 NPP 2.1(ea) deals specifically with genetic information that has been collected in the course of providing a health service to an individual and allows an organisation to use or disclose that information to a genetic relative where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of the genetic relative. NPP 2.1(ea) also provides that any such use or disclosure must be in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner.[78]

60.65 NPP 2.4 establishes a regime under which a health service provider may disclose an individual's health information to 'a person who is responsible for the individual' including certain family members, carers and legal guardians in some circumstances. These include where the individual is physically or legally incapable of giving consent to the disclosure.[79]

60.66 NPP 6.1(b) provides a special exception to the access principle in relation to health information. An organisation need not provide access to an individual's health information where providing access would pose a serious threat to the life or health of any individual. In these circumstances the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.[80]

The draft National Health Privacy Code

60.67 In June 2000, Australian Health Ministers established the Australian Health Ministers' Advisory Council (AHMAC) National Health Privacy Working Group. The purpose of the Working Group was to address the need for a nationally consistent framework for health information privacy. The AHMAC Working Group was made up of representatives of state and territory health authorities and the Australian Government Attorney-General's Department; and was chaired by DOHA. The Health Insurance Commission, the Australian Institute of Health and Welfare and the OPC had observer status on the AHMAC Working Group and provided specialist advice.[81]

---

77 NPP 10.2 is discussed further in Ch 63.

78 This provision implements Rec 21–1 of Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003). NPP 2.1(ea) is discussed further in Ch 63.

79 NPP 2.4 is discussed further in Ch 63, and in Ch 70 in relation to adults with a decision-making disability.

80 NPP 6.1(b) is discussed further in Ch 63.

81 Phillips Fox, *Report on Public Submissions in Relation to Draft National Health Privacy Code* (2003), 1.

60.68 The framework developed by the AHMAC Working Group has become known as the draft *National Health Privacy Code* (the draft Code). In order to achieve national consistency, the draft Code was intended to apply to all health service providers and organisations that collect, hold or use health information across the public and private sectors in every Australian state and territory.[82] The draft Code contains 11 National Health Privacy Principles (NHPPs) and additional detailed procedures for providing individuals with access to their health information.

60.69 Following a public consultation process, a revised version of the draft Code, as well as draft mandatory research guidelines and explanatory notes for the use or disclosure of genetic information, were developed.[83] These, however, have not been made available publicly. Consequently, where provisions of the draft Code are discussed in this Report, references are to the provisions released for public comment in 2003. While much of its content was finalised, as at August 2006 the draft Code had not been endorsed formally at a ministerial level[84] and an implementation mechanism had not been settled.[85]

60.70 Although the NHPPs have much in common with the NPPs, there are also numerous differences. In general, the NHPPs are more detailed and provide specific guidance on issues such as the handling of health information on the death of a health service provider or where a health service closes, is sold or amalgamates with another service. Some specific NHPPs differ from their equivalent NPPs. For example, while NPP 4 requires organisations to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed,[86] NHPP 4 requires health service providers to retain health information for at least seven years.[87]

State and territory health privacy legislation

60.71 The *Health Records and Information Privacy Act 2002* (NSW) regulates the handling of health information in the public and private sectors and includes a set of 15 Health Privacy Principles (HPPs). The HPPs expressly address issues such as the use of health information without consent for: the funding, management, planning or evaluation of health services;[88] research;[89] and health records linkage.[90] The Act also includes detailed provisions on providing access to health information.

---

82 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 1 cl 1, pt 2 div 2.

83 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

84 Australian Government Department of Health and Ageing, *Correspondence*, 17 August 2006.

85 National E-Health Transition Authority, *NEHTA's Approach to Privacy*, Version 1.0 (2006).

86 *Privacy Act 1988* (Cth) sch 3, NPP 4.2.

87 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 4.2.

88 *Health Records and Information Privacy Act 2002* (NSW), sch 1, HPP 10(1)(d).

89 Ibid sch 1, HPP 10(1)(f).

60.72 The *Health Records Act 2001* (Vic) also regulates the handling of health information in the public and private sectors and includes a set of 11 HPPs. The Victorian HPPs require the retention of health information records for at least seven years.[91] The HPPs also expressly address issues such as: the use of health information without consent in the funding, management, planning, monitoring, improvement or evaluation of health services;[92] the use of health information in research;[93] the transfer of health information when a consumer changes health service provider; and arrangements for the custody of health information when a health service provider closes or dies.[94] As in New South Wales, the Act includes detailed provisions on providing access to health information.

60.73 The *Health Records (Privacy and Access) Act 1997* (ACT) regulates the handling of health information in the public and private sectors and includes a set of 12 Privacy Principles. These principles expressly address issues such as: the sharing of information among members of a treating team;[95] transfer or closure of a health service provider's practice; and the transfer of a health consumer's health information from one health service provider to another when the consumer changes health service provider.[96] In common with the legislation in New South Wales and Victoria, the Act includes detailed provisions on providing access to health information.

Issues Paper 31

60.74 In IP 31, the ALRC asked whether the draft *National Health Privacy Code* was an effective away to achieve a nationally consistent and appropriate regime for the regulation of health information.[97] Implicit in this question was the question of whether the handling of health information requires a separate and distinct set of principles.

Submissions and consultations

60.75 In consultation, the Office of the Health Services Commissioner (Victoria) expressed the view that health information does require a separate set of principles because of the intimate nature of the information and the fact that some health information—such as mental health information—can lead to stigmatisation or discrimination.[98] In its submission, the Office of the Health Services Commissioner also expressed the view that the draft Code provided a good starting point:

> A great deal of important work and consultation with key stakeholders has already taken place. It would be a regrettable waste of public resources not to utilize the work

90 Ibid sch 1, HPP 15.
91 *Health Records Act 2001* (Vic) sch 1, HPP 4.
92 Ibid sch 1, HPP 2.2(f).
93 Ibid sch 1, HPP 2.2(g).
94 Ibid sch 1, HPP 10.
95 *Health Records (Privacy and Access) Act 1997* (ACT) sch 1, Privacy Principles 9 and 10.
96 Ibid sch 1, Privacy Principles 11 and 12.
97 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–3.
98 Victorian Government Office of the Health Services Commissioner, *Consultation PC 28*, Melbourne, 9 May 2006.

> involved in drafting the *National Code*. Mirror or applied legislation as set out in paragraph 8.43 of the Issues Paper are the most desirable and effective models for implementing the *National Code*.[99]

60.76 A number of other stakeholders agreed that health information and the health services context are unique and require a specific regulatory regime.[100] Some stakeholders expressed support for the draft Code.[101]

60.77 The Australian Nursing Federation stressed the need for consistent and carefully crafted principles to assist health service providers to achieve the difficult balances that are required in their daily decision making. The Federation also noted the considerable investment in the development of the draft *National Health Privacy Code* and expressed the view that the draft Code was an appropriate vehicle for developing a nationally consistent framework for the regulation of health information.[102]

60.78 The Western Australian Department of Health expressed support for a separate set of health principles, noting the need to use health information for continuity of care in relation to individuals and monitoring and protecting the community on public health issues. The Department noted, however, that a separate set of principles may lead to uncertainty in some contexts—such as child welfare—about which principles apply.[103]

60.79 On the other hand, a significant number of other stakeholders were of the view that, for simplicity and consistency, one set of privacy principles should apply to personal information, including health information. There was recognition, however, that there may be a need for supplementary principles or guidance on the detailed application of the principles in the health services context.[104]

---

99 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

100 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Council of Social Service of New South Wales, *Submission PR 115*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

101 Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007.

102 Australian Nursing Federation, *Submission PR 205*, 22 February 2007.

103 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

104 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Health and Community Services Complaints Commission (South Australia), *Submission PR 207*, 23 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; South Australian Government Department of Health, *Consultation PC 113*,

60.80 The NHMRC expressed some support for the draft *National Health Privacy Code*, but stated that it would prefer a uniform national system incorporating specific elements regulating health information, rather than a separate code.[105] The OPC agreed with the NHMRC, stating that:

> Health privacy regulation could be enhanced by building upon existing provisions, without the necessity of an additional instrument or an entirely new set of principles.
>
> The Office understands that other stakeholders may hold differing views on this matter and would prefer a separate regulatory instrument specifically for the health sector. The Office submits that a uniform and coherent approach to privacy regulation is best served by incorporating privacy protections into a single body of regulation.
>
> A single body of regulation is also likely to reduce regulatory complexity for those agencies and organisations that handle both health and non-health information. The existence of separate sets of principles may create confusion by requiring agencies and organisations to refer to different instruments, depending on the type of personal information they are handling at any given time.[106]

60.81 In the course of the OPC Review, the OPC considered whether it would be possible to incorporate elements of the draft Code into the NPPs. The OPC stated that

> the resulting principles would be longer and more complex. This option would require the insertion of multiple sub-principles and exceptions to the NPPs to take account of the code.
>
> This approach would run counter to the intent of delivering general, high-level principles for all business and government sectors. For instance, the approach would mean that non-health organisations and agencies would need to deal with a more complex set of privacy principles, where much of the content may not apply to them. This would not improve, and may even increase, regulatory complexity overall.[107]

60.82 In addition, the OPC stated in its submission on IP 31 that the draft *National Health Privacy Code* seemed 'unwieldy, complex and overly prescriptive'.[108]

60.83 The Australian Privacy Foundation stated that, while in principle the draft Code could form the basis of more detailed principles for health information:

> One difficulty with the development of a separate code is that it encourages drafters and stakeholders to adjust the information privacy principles more than necessary, creating arbitrary or intricate differences that then create confusion. This is evident in the creation of the *Health Records Act* in Victoria, which adopts much of the information privacy principles that appeared in the State's *Information Privacy Act*

Adelaide, 2 March 2007; Australasian Compliance Institute, *Consultation PC 53*, Sydney, 17 January 2007; B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

105 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

106 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

107 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 70.

108 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

but is more prescriptive and creates distinctions that may or may not be significant yet cause confusion.[109]

Discussion Paper proposals

60.84 In DP 72, the ALRC expressed the view that health information should be regulated under the general provisions of the *Privacy Act* and the UPPs. Certain additions to the proposed UPPs, relating specifically to the handling of health information, were to be promulgated in new regulations under the *Privacy Act*—the *Privacy (Health Information) Regulations.*[110] Some of these proposed regulations were based on elements of the draft *National Health Privacy Code* and are discussed in detail in Chapter 63. The intent of the proposal was to capture those elements of the draft Code that stakeholders considered most valuable and to build them into a system based on the *Privacy Act* and the UPPs. This was intended to ensure that the principles regulating personal information and health information were the same, as far as possible. The additional provisions dealing with health information, to be set out in the new regulations, were designed to sit comfortably with the UPPs.

60.85 The ALRC also proposed that the OPC should publish a document bringing together the UPPs and any health-specific additions set out in the regulations.[111] It was intended that this document would contain a complete set of UPPs and regulations relating to health information. Finally, the ALRC proposed that the OPC—in consultation with DOHA and other relevant stakeholders—should develop guidelines on the handling of health information under the *Privacy Act* and regulations.[112]

Submissions and consultations

60.86 These proposals received a mixed response in submissions and consultations. A number of stakeholders expressed the view that the proposed regulatory structure had the potential to lead to confusion, as agencies and organisations handling health information would be required to consider both the UPPs and the regulations.[113] Another stakeholder was concerned that the proposed framework would not support national consistency.[114]

60.87 The Victorian Office of the Health Services Commissioner remained of the view that a separate set of health privacy principles was necessary. The Office also stated that high-level principles are sometimes not sufficient for dealing with the handling of

---

109 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.
110 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 56–2.
111 Ibid, Proposal 56–3.
112 Ibid, Proposal 56–4.
113 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; Pharmacy Guild of Australia, *Submission PR 433*, 10 December 2007.
114 Confidential, *Submission PR 570*, 13 February 2008.

health information and that more prescriptive rules are necessary in some circumstances. The Office noted that rules-based regulation does not have an adverse effect on cooperative, compliant organisations and provides certain and enforceable provisions where necessary.[115]

60.88 On the other hand, the Government of South Australia was of the view that the model UPPs would provide sufficient protection for health information and that additional regulations would be unnecessary. If there was a need for additional provisions, the Government of South Australia was of the view that they should be included in the UPPs.[116] The OPC agreed that any additional provisions should be included in the body of the UPPs.[117]

60.89 The Australian Privacy Foundation expressed support for the proposals, while expressing some concern about the complexity of the ALRC's proposed regulatory framework and the efficacy and balance of OPC guidance.[118] Other stakeholders expressed support for the ALRC's proposed regulatory structure.[119] The Centre for Law and Genetics expressed support, noting that the proposals

> seek to maximise achieving consistency of the revised federal principles (proposed UPPs) but at the same time, acknowledging the special considerations pertaining to the health area. We believe that this will adequately cater for the practical needs of this complex area without detracting from a coherent national privacy scheme in Australia.[120]

60.90 The Australian Government Department of Human Services noted that the proposed approach would provide certainty in terms of requirements, and administrative flexibility where health-specific amendments to the UPPs were necessary.[121]

---

115 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.
116 Government of South Australia, *Submission PR 565*, 29 January 2008.
117 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
118 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
119 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Northern Territory Government Department of Health and Community Services, *Submission PR 480*, 17 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
120 Centre for Law and Genetics, *Submission PR 497*, 20 December 2007.
121 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

60.91 There was significant support for the ALRC's proposal that the OPC develop guidance on the handling of health information,[122] with a number of stakeholders noting that the consultation process should involve state and territory agencies, health service providers, health insurers, health consumers and others.[123] Carers Australia noted that this guidance could assist health service providers to engage and share information with carers in appropriate circumstances.[124]

ALRC's view

60.92 The ALRC recognises that handling health information does raise some unique issues and that these require additional consideration in the development of privacy principles, rules and guidelines. For example, in ALRC 96, the ALRC and AHEC noted:

> The collection of family medical history is an established part of medical practice. When providing a health service, health professionals may need to collect family medical history in order to diagnose a patient's condition accurately ... If this information is not collected the medical care or advice provided to the patient may be compromised.[125]

60.93 The ALRC also acknowledges the investment of time and effort that has gone into developing the draft *National Health Privacy Code* and the level of support the draft Code has among stakeholders. The provisions of the draft Code, taken as a whole, are very detailed and highly prescriptive. As discussed in Chapter 4, the ALRC's preference is for principles-based regulation as the foundation of privacy regulation in Australia, only relying on more prescriptive rules where absolutely necessary.

60.94 Chapter 4 examines the differences between principles-based regulation and prescriptive rules-based regulation. Principles-based regulation sets out objectives without providing inflexible rules on how to achieve those objectives. Principles-based regulation provides greater flexibility, enabling the regime to respond to new issues as they arise without having to create new rules. Rules-based regulation is less flexible

---

122 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Northern Territory Government Department of Health and Community Services, *Submission PR 480*, 17 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007 ; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

123 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

124 Carers Australia, *Submission PR 423*, 7 December 2007.

125 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [21.4].

and can impose requirements that are not always appropriate in every situation. The draft Code includes a significant amount of material that is closer in nature to rules than principles, setting out how health information is to be handled in particular situations. For example, the Code includes 17 clauses on access to health information. This level of detail is not necessary and has the potential to stymie creative approaches to providing access to health information.

60.95 The 'Access and Correction' principle, discussed in Chapter 29, provides a suggested framework for access to personal information. Much of the detail provided in the draft Code in relation to access—for example, how a right of access may be exercised and in what form health information may be provided—is consistent with this principle and could be included in guidelines issued by the OPC. The guidelines could make clear, for example, that organisations may provide a copy of the health information to the individual or, if the individual agrees, an accurate summary of the health information.[126] The ALRC recommends that the OPC develop such guidelines in consultation with relevant stakeholders and is of the view that the draft Code would provide a valuable starting point in the development of such guidelines.

60.96 In addition, the ALRC is strongly of the view that it is undesirable to have two sets of privacy principles, one set dealing with health information and one set dealing with other personal information. In Chapter 14, the ALRC examines the impact of inconsistency and fragmentation in the privacy regime and notes that one cost is less sharing of information in appropriate circumstances. This is a particular problem in the health services context where appropriate sharing of health information between members of treating teams is essential to the wellbeing of health consumers.

60.97 The Taskforce on Reducing Regulatory Burdens on Business (the Regulatory Taskforce) noted that achieving nationally consistent privacy laws is an important factor in reducing compliance costs for business.[127] The Regulatory Taskforce recommended that the Australian Government ask the Standing Committee of Attorneys-General to endorse national consistency in all privacy-related legislation based on the concept of minimum effective regulation.[128] In its response to *Rethinking Regulation*, the Australian Government stated that:

> The Australian Government agrees to the recommendation and supports the goal of national consistency in privacy-related legislation. At the April 2006 meeting of the Standing Committee of Attorneys-General, Attorneys-General agreed to establish a working group to advise Ministers on options for improving consistency in privacy regulation, including workplace privacy.[129]

---

126 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 5, div 1, cl 3(1)(b).

127 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), [4.151].

128 Ibid, rec 4.47.

129 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

60.98 Having one set of principles regulating the handling of health information and another set of principles regulating the handling of other personal information would not reduce compliance costs for business and would not be consistent with the goal of national consistency in privacy legislation. The provisions of the draft Code are not consistent with the provisions of the *Privacy Act*, or with the model UPPs. Having two regimes running side by side would contribute to fragmentation, inconsistency and compliance costs for all stakeholders, particularly those who handle both health and non-health information.

60.99 Health information is handled in a range of contexts, not only the health services context. Agencies and organisations that handle health information as well as other personal information should not be required to comply with two sets of principles. There is significant overlap in the basic approach to handling health information in state and territory legislation, the NHPPs and the model UPPs. For example, UPP 5 provides that sensitive information, including health information, may be used for the purpose for which it was collected or a directly related secondary purpose where the individual would reasonably expect the information to be used in that way. This is consistent with the Victorian HPPs and the NHPPs. The NSW HPPs and the ACT privacy principles only require that the secondary purpose be directly related to the purpose for which it was collected.

60.100 The model UPPs provide a suitable basic framework for handling health information. With some health-specific additions to the UPPs, a single legislative scheme would work effectively to regulate both health information and other personal information. These additions, including some health-specific exceptions to the UPPs and a number of health-specific additional privacy principles, are discussed in Chapter 63 and include some of the provisions developed in the context of the draft *National Health Privacy Code.*

60.101 The ALRC has considered whether the health-specific principles and exceptions should sit within the UPPs or outside the UPPs. Each approach has advantages and disadvantages. If the additional elements were included in the UPPs, the UPPs would be longer and more complex, but agencies and organisations would only have to refer to one source of guidance in handling all personal information, including health information. On balance, however, the ALRC recommends that the additional health information principles and exceptions to the UPPs be set out in regulations to be called the *Privacy (Health Information) Regulations*. This means that, for those agencies and organisations that do not handle health information, the UPPs will be more concise and accessible.

60.102 For those agencies and organisations that do handle health information, the ALRC recommends that the OPC publish a document setting out the UPPs as amended by the new *Privacy (Health Information) Regulations*. This document will provide a complete set of privacy principles covering health information, as well as other

personal information. It would be possible to include a note in the UPPs indicating that those agencies and organisations that handle health information should refer to the *Privacy (Health Information) Regulations.*

60.103 The other reason that the ALRC proposes that health information-specific principles and exceptions be included in regulations is that health is an area in which the application of the model UPPs may need to be modified or clarified from time to time. In 2006, for example, the NPPs were amended to provide for the use and disclosure of genetic information to lessen or prevent a serious threat to the life, health or safety of a genetic relative.[130] This kind of change is achieved more easily through regulation, than by amendment of the UPPs in the principal Act.

Recommendation 60–1 Health information should be regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles (UPPs), and regulations under the *Privacy Act*—the new *Privacy (Health Information) Regulations.* The new *Privacy (Health Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model UPPs.

Recommendation 60–2 The Office of the Privacy Commissioner should publish a document bringing together the model Unified Privacy Principles (UPPs) and the additions set out in the new *Privacy (Health Information) Regulations*. This document should contain a complete set of the model UPPs as they relate to health information.

Recommendation 60–3 The Office of the Privacy Commissioner—in consultation with the Department of Health and Ageing and other relevant stakeholders—should develop and publish guidelines on the handling of health information under the *Privacy Act* and the new *Privacy (Health Information) Regulations*.

130 *Privacy Legislation Amendment Act 2006* (Cth).

61. Electronic Health Information Systems

Contents

Introduction

61.1 Traditionally, health information has been collected and stored in paper-based systems, with information about one individual held in a number of disparate locations, such as general practitioners' records, hospital records, and medical specialists' records. Increasingly, however, health information is collected, stored and transferred in electronic form and health information about large numbers of health consumers is collected into central databases, such as the Medicare database and cancer registers. Another important trend is the move to integrate health information systems and to create shared electronic health records. Sharing and linking of health information about particular health consumers has the potential to achieve better public and private health outcomes by allowing health service providers better access to health information. It also gives rise to privacy concerns.

61.2 In this chapter, the ALRC considers these developments and concludes that the collection of health information into electronic health information systems does not require specific legislative control, provided that the *Privacy Act* is updated and amended as recommended in this Report. The Australian Government proposal to establish national shared electronic health records (SEHR) based on a unique healthcare identifiers (UHIs) system, to be developed separately, however, should be based on specific enabling legislation. The linking of electronic health information for the purposes of research is discussed in Chapter 66.

Background

Electronic health information systems

61.3 A large number of electronic health information systems are being developed at local, regional, state and territory, and national levels across Australia. Many of these systems are being developed within the federal Health*Connect* framework. Health*Connect* is

> an overarching national change management strategy to improve safety and quality in health care by establishing and maintaining a range of standardised electronic health information products and services for health care providers and consumers.[1]

61.4 In its submission to the Office of the Privacy Commissioner (OPC) review of the private sector provisions of the *Privacy Act 1988* (Cth) (the OPC Review), the Department of Health and Ageing (DOHA) stated that Health*Connect* was designed to overcome gaps in information flow at the point of clinical care and that:

> While there is wide acceptance of the benefits that Health*Connect* can deliver, particularly in the areas of patient safety and quality of care, there is also recognition that there are privacy and security risks that need to be managed to ensure such benefits are realised. Personal health information is sensitive information, and both consumers and providers will need to have trust in how their information is handled within and external to Health*Connect* ahead of participating in this system. In this context, privacy and security issues are consistently identified as a key building block for Health*Connect* among all stakeholders.[2]

61.5 The following are examples of electronic health information initiatives being developed at the state level. In March 2006, the New South Wales Government announced Health*elink*, an electronic health records system which is currently being piloted in different parts of the state. Health*elink* brings together a summary of an individual's health information from different doctors, hospitals and other health service providers into one secure computer record.[3] Health*Connect* Northern Territory has also commenced implementation of a shared electronic health record service.[4] Health*Connect* South Australia is working on three major initiatives, including the development of an electronic planning and referral system for health consumers with chronic disease.[5]

---

1 Australian Government Department of Health and Ageing, *HealthConnect: FAQs* <www.healthconnect.gov.au> at 14 May 2008.

2 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

3 J Hatzistergos (New South Wales Minister for Health), 'Trial of Electronic Health Records' (Press Release, 23 March 2006).

4 C Burns (Northern Territory Minister for Health), 'Connecting Health Services Territory-Wide' (Press Release, 1 November 2006).

5 HealthConnect South Australia, *HealthConnect South Australia: Health Information When You Need It* <www.healthconnectsa.org.au/> at 14 May 2008.

61.6 The Health*Connect* website notes that there are a number of national initiatives under development that could be implemented within the next 12 to 18 months, including:

- e-prescriptions—prescriptions for medication being sent electronically from health care providers to pharmacies;
- e-referrals—referrals or requests being sent electronically from one health care provider to another (for example, from a doctor to a radiologist); and
- hospital discharge summaries—summaries of the treatment provided and the proposed future care plan being sent electronically from hospitals to doctors, specialists or aged care facilities.[6]

61.7 The National E-Health Transition Authority (NEHTA) was established in 2005 to set national standards, specifications and infrastructure requirements for electronically collecting and securely exchanging health information. NEHTA is funded jointly by the Australian, state and territory governments. The NEHTA Board is composed of the chief executive officers of the Australian, state and territory health departments. The aim is to ensure a common national approach, setting the necessary foundations for future electronic health systems across Australia.[7]

National shared electronic health records

61.8 In February 2006, the Council of Australian Governments (COAG) agreed to accelerate work on a national electronic health records system

> to build the capacity for health providers, with their patient's consent, to communicate quickly and securely with other health providers across the hospital, community and primary medical settings.[8]

61.9 NEHTA is responsible for developing a design for a national approach to Shared Electronic Health Records (SEHRs)—records that will contain selected health information about a health consumer, which can be shared among multiple authorised health service providers. An important precursor to SEHRs is the development of a Unique Healthcare Identifiers (UHIs) scheme for individuals and healthcare providers to ensure that information is attributed to the right patient and the right provider.

---

6 Australian Government Department of Health and Ageing, *HealthConnect: FAQs* <www.healthconnect .gov.au> at 14 May 2008.

7 National E-Health Transition Authority, *About NEHTA* <www.nehta.gov.au> at 1 August 2007.

8 Council of Australian Governments, *Council of Australian Governments' Communique*, 10 February 2006. The Commonwealth agreed to contribute $65 million to the project and the states and territories agreed to contribute $65 million in the period to 30 June 2009.

> Healthcare requires the constant collection, exchange and transmission of health information. This is usually in the context of information about a single patient being exchanged between multiple healthcare providers. It is critical for patient safety and privacy that this information exchange occurs reliably and securely.
>
> The Council of Australian Governments has committed Australia to a single, national approach to identifying individuals and healthcare providers for the purposes of health communications. This approach, being developed by NEHTA, is known as the Unique Healthcare Identification (UHI) Service.
>
> The UHI Service will involve the allocation, issuing and maintenance of unique identifiers for individuals (known as the Individual Healthcare Identifier or IHI) and healthcare providers (the Healthcare Provider Identifier or HPI).[9]

61.10 In December 2006, NEHTA released a *Privacy Blueprint—Unique Healthcare Identifiers*,[10] which discusses how NEHTA proposes to manage the privacy issues arising from the UHI Service. The *Privacy Blueprint* states that the Individual Healthcare Identifier (IHI) will be used only to identify individuals for health care and that individuals will not be required to produce an IHI to receive health care.[11] NEHTA also expresses the view that legislation supporting the creation of the UHI Service would create greater legal certainty, particularly around the creation and distribution of unique identifiers. Other issues that might be covered in such legislation include governance arrangements and sanctions for misuse of the identifiers.[12]

61.11 A report on feedback to the *Privacy Blueprint—Unique Healthcare Identifiers*, noted that:

> Any unique personal identifier, especially where widely held in the community, raises a significant privacy risk of inappropriate datalinking and data-matching. The OPC noted that it will be important to ensure this risk is mitigated and that such a highly reliable identifier is not usurped for purposes beyond the health system and the clinical care of individuals.
>
> The UHI Service potentially holds a very large database on most, if not all, Australians and foreign residents who obtain healthcare. The OPC considered a unique aspect of the proposal is that access to UHI data will be available to a large number of health sector users, raising the risk of misuse or abuse of the data and access privileges, particularly to locate the home address of an individual for purposes unrelated to healthcare. Accordingly, the OPC welcomed NEHTA's detailed measures contained in the Privacy Blueprint directed at protecting individual privacy.[13]

---

9 National E-Health Transition Authority, 'Privacy Blueprint—Unique Healthcare Identifiers Release Notes' (Press Release, 13 December 2006). Identifiers are discussed in detail in Ch 30.

10 National E-Health Transition Authority, *Privacy Blueprint—Unique Healthcare Identifiers*, Version 1.0 (2006).

11 National E-Health Transition Authority, 'Privacy Blueprint—Unique Healthcare Identifiers Release Notes' (Press Release, 13 December 2006).

12 National E-Health Transition Authority, *Privacy Blueprint—Unique Healthcare Identifiers*, Version 1.0 (2006), 24.

13 National E-Health Transition Authority, *Privacy Blueprint on Unique Healthcare Identifiers: Report on Feedback*, Version 1.0 (2007), 5.

61.12 The OPC Review recommended that the Australian Government consider developing specific enabling legislation to underpin any national electronic health records system. The Review also recommended that any such legislation should include safeguards to ensure that participation in the system is voluntary, and limitations on the use of the records in the system.[14]

Issues Paper 31

61.13 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or the draft *National Health Privacy Code*.[15] Submissions in response to IP 31 drew a distinction between electronic health information systems that simply stored health information in electronic form or transmitted information in electronic form, and those systems that centralised an individual's health information and allowed a number of different health service providers to access that information—in particular, the proposal to develop a national SEHR scheme.

Electronic health information systems

61.14 In its submission, the Western Australian Department of Health noted that:

> Electronic health information systems pose risks to privacy because of the speed and reach of information transfer. However, they also provide new opportunities to increase individual control and to improve security and the ability to audit access to information. Arguably, the privacy issues with electronic systems are not different in kind from those relating to paper-based systems of information storage and general principles are usually appropriate. However, the principles must be informed by a thorough knowledge of electronic storage and transfer practices.[16]

61.15 The Office of the Information Commissioner (Northern Territory) agreed that high-level privacy principles should be sufficient.

> The *Privacy Act* and privacy principles do not, and should not, attempt to prescribe detailed requirements for any particular project. They operate at a higher level. Likewise, a national code would operate at a high level and should be reviewed only infrequently. It would be inappropriate to single out electronic health systems for prescriptive treatment that may prove unable to cope with technological changes that appear in a few years time.[17]

---

14 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 71.

15 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–5.

16 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

17 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

61.16 The Victorian Office of the Health Services Commissioner stated that the provisions of the *Health Records Act 2001* (Vic) deal adequately with electronic health information systems.[18]

National shared electronic health records

61.17 In its submission, DOHA acknowledged that:

> National e-health systems such as Unique Health Identifiers (UHIs) and the Shared Electronic Health Record (SEHR) will significantly change the way health information is handled in the provision of healthcare services. They will lead to greater aggregation of health information which is more searchable. More information about an individual will be potentially available to many more people. The development of these systems will create new opportunities over time for examining this information for the benefit of the individual concerned and the community as a whole, but also carry the possibility of misuse.[19]

61.18 DOHA noted that, for these systems to realise their potential benefits, a high level of public trust and confidence will be necessary. DOHA was of the view that specific legislation providing clarity, certainty, and predictability will be necessary to build and maintain this trust and confidence. In DOHA's view, legislation should set out the purposes and permitted uses of UHIs and SEHRs and, in addition, could address the following issues:

- the establishment of a standing governance body or bodies to oversight the management and operation of specified e-health systems;
- who has control over the information collected and how this will be exercised;
- eligibility criteria, rights and requirements for participation in specified e-health systems by consumers and providers;
- limitations on the personal information that may be collected in relation to specified e-health systems;
- the rights of individuals to exercise control over information held about them and to access and correct this information;
- restrictions on the use or disclosure of the information collected and any penalties for improper use or disclosure;
- rules and decision-making processes governing the secondary use of information;
- prohibitions on function creep or the mechanisms to authorise any changes in use;
- arrangements for ensuring data quality and security of records containing personal information;

---

18 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

19 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

- arrangements for access to records and audit logs by the individual concerned or their authorised representative;
- remedies for improper access and use, including complaints mechanisms; and
- arrangements for enforcing compliance with the standards for interoperability in the healthcare sector that are proposed to be published by the National E-Health Transition Authority (NEHTA).[20]

61.19 In its submission, the OPC also considered the proposal to establish SEHRs and expressed the view that such systems 'should be accompanied by specific legislative measures to ensure community confidence that personal health information will be handled privately'.[21] In the OPC's view, such legislation should provide for:

- participation on an opt-in basis;
- the primary uses of data;
- a designated authority and processes for approval of secondary uses of data;
- consent processes; and
- sanctions and complaint mechanisms.

61.20 NEHTA submitted that it may be desirable to develop specific legislation to support these new initiatives where they raise issues that fall outside the ambit of statutory privacy regimes, such as governance.[22]

Discussion Paper proposals

Electronic health information systems

61.21 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC expressed the view that the collection of health information into electronic health information systems does not necessarily require specific legislative control if the *Privacy Act* is updated and amended, as proposed in DP 72. The collection of health information into stand-alone electronic records, and the use of electronic systems to transmit health information among health service providers treating an individual, do not raise new or unique issues. The model Unified Privacy Principles (UPPs) and the new *Privacy (Health Information) Regulations* are intended to be technology neutral and will regulate satisfactorily the handling of electronic health information in these circumstances.

---

20 Ibid.
21 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
22 National E-health Transition Authority, *Submission PR 145*, 29 January 2007.

National shared electronic health records

61.22 The ALRC expressed the view, however, that the establishment of a national UHI or SEHR scheme would require specific enabling legislation. The ALRC recognised the significant potential benefits to healthcare quality and safety that the establishment of such schemes may deliver, but noted that such schemes will work effectively only if there is a sufficient degree of public trust and public confidence in the schemes and their administration. The ALRC also expressed the view that national developments of such importance involving the establishment and use of unique identifiers for all Australians, and the development of a national approach to SEHRs, should be subject to comprehensive public debate and parliamentary scrutiny.

61.23 The ALRC agreed with NEHTA's position that enabling legislation should deal with those issues that fall outside existing privacy regulation. The ALRC proposed that such enabling legislation should nominate or establish an agency or organisation with clear responsibility for managing the UHI and SEHR schemes; set out eligibility criteria, rights and requirements for participation in the schemes, including consent requirements; specify the permitted and prohibited uses and linkages of the personal information held in the systems and the permitted and prohibited uses of UHIs; establish sanctions in relation to misuse; and include specific safeguards, for example, that it is not necessary to use a UHI in order to access health services.[23]

61.24 The ALRC proposed, however, that the systems should remain subject to the *Privacy Act* and the proposed UPPs as amended by the proposed *Privacy (Health Information) Regulations*.

Submissions and consultations

61.25 In response to DP 72, the Australian Privacy Foundation expressed opposition to the establishment of a centralised health information system, based on unique identifiers. It argued that such a system posed an unacceptable risk to the privacy of health information and was unnecessary. The Australian Privacy Foundation's view was that a more appropriate approach would be a federated model where separate systems were linked in specific circumstances and subject to safeguards. The Australian Privacy Foundation stated that:

> The Foundation urges that the ALRC not reach any conclusions, and not make any recommendations, that pre-suppose that centralised data schemes or a universal identifier are even desirable, let alone inevitable.
>
> The Foundation further submits that the ALRC should expressly recognise that strong arguments exist against those approaches and in favour of federation among large numbers of independent databases, and should frame its conclusions and recommendations in order to reflect the unsettled nature of health care data architectures.[24]

---

23 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 56–5.

24 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

61.26 Microsoft Asia Pacific also supported a federated model:

> Microsoft considers that a privacy-sensitive approach to the development of electronic health information management systems would be to adopt a federated data model. Rather than centralising data storage, a federated model seeks to centralise the point of access. Data storage is compartmentalised and access is granted only on a 'need to know' basis. This approach ensures that systems are designed with built-in checks and balances to lower the risk (both in terms of the likelihood and magnitude) of data security breaches.[25]

61.27 The Australian Institute of Health and Welfare (AIHW) expressed the view that, although the SEHR and UHI schemes differ from existing electronic health records and identifiers in scale, they are not different in nature. In the AIHW's view, creating separate provisions to regulate the schemes would result in inconsistency.[26]

61.28 On the other hand, the Australian Privacy Foundation, and a number of other stakeholders, were of the view that specific legislation would be required if projects of the scale and scope of the proposed SEHR and UHI schemes were to go forward.[27] Medicare Australia noted that:

> The COAG funding approval for the UHI was predicated on leveraging the personal information stored in Medicare Australia's Consumer Directory for the initial data load to populate the Individual Healthcare Identifier (IHI) portion of the UHI system. It will therefore be essential for the enabling legislation to provide the specific authority to use the Medicare data in that way.
>
> Given the significance of these programs to the vast majority of the public, it is particularly appropriate that the framework be subject to public debate and parliamentary scrutiny.
>
> In developing the legislation, we think the most important factor will be to ensure that consumers can effectively control the handling of their personal information.[28]

61.29 The Victorian Office of the Health Services Commissioner agreed that enabling legislation would be required for the schemes, but was of the view that a separate set of health privacy principles was also necessary and should apply to the schemes.[29]

---

25 Microsoft Asia Pacific, *Submission PR 463,* 12 December 2007.
26 Australian Institute of Health and Welfare, *Submission PR 552,* 2 January 2008.
27 Confidential, *Submission PR 570,* 13 February 2008; Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Medicare Australia, *Submission PR 534,* 21 December 2007.
28 Medicare Australia, *Submission PR 534,* 21 December 2007.
29 Office of the Health Services Commissioner (Victoria), *Submission PR 518,* 21 December 2007.

61.30 A number of other stakeholders expressed general support for the ALRC's proposed approach.[30] The OPC expressed support for the proposal and noted that it had provided a submission to NEHTA concerning its *Privacy Blueprint for Unique Health Identifiers*.

> This submission raised a number of privacy risks, including the risks posed by the backend UHI Service database. As the Office understands the proposal, this database would be a national database of names and addresses of individuals with UHIs. The Office noted that while other similarly large databases exist in Australia, such as those maintained by Medicare Australia and the Australian Taxation Office, what would seem to make this repository unique is the potential for it to be accessible to a large number of users who work in the health sector. In regard to privacy protections, users will interact with the database in different jurisdictions, some of which may have no privacy legislation.[31]

ALRC's view

61.31 A number of stakeholders expressed the view that a centralised shared health records system based on unique identifiers is not the best way forward. The ALRC expresses no view on whether a centralised or federated model is preferable. Such concerns are, however, one reason that any such scheme should be underpinned by specific enabling legislation. The development and passage of such legislation will provide an opportunity, although not the only opportunity, for public scrutiny of, and debate on, the proposed scheme.

61.32 Any such legislation should deal with those issues that fall outside existing privacy regulation and provide more stringent rules where necessary. The legislation should, for example, nominate or establish an agency or organisation with clear responsibility for managing the systems, including the privacy of personal information in the systems. There should be clear lines of accountability. The legislation should set out the permitted and prohibited uses of UHIs and sanctions for misuse. Moreover, the legislation should make absolutely clear that certain safeguards are fundamental; for example, that it is not necessary to use a UHI to access health care.

61.33 As discussed in Chapter 30, legislative schemes establishing multi-purpose identifiers—such as UHIs—will also need to address the issues raised by the 'Identifiers' principle. The 'Identifiers' principle prohibits the adoption, use and disclosure by organisations of multi-purpose identifiers except in certain circumstances.[32] It will be necessary to set out in the legislation establishing the UHIs—or in regulations under the *Privacy Act*—those organisations allowed to adopt,

---

30 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Northern Territory Government Department of Health and Community Services, *Submission PR 480*, 17 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

31 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

32 UPP 10.3.

use and disclose UHIs, and the circumstances in which it is lawful for those organisations to do so. In addition, the ALRC has recommended that, before the introduction by agencies of any unique multi-purpose identifier, such as the UHI, the Australian Government, in consultation with the Privacy Commissioner, should conduct a privacy impact assessment.[33]

61.34 The systems should remain subject to the *Privacy Act* and the model UPPs as amended by the new *Privacy (Health Information) Regulations*. For example, health information generally should be collected for inclusion in an SEHR with consent. That information should be used or disclosed only for the purpose for which it was collected or a directly related secondary purpose where the individual would reasonably expect the agency or organisation to use or disclose the information for that purpose. Exceptions in the UPPs and the regulations would apply so that, for example, it would be possible to use or disclose an individual's health information held in an SEHR if the agency or organisation reasonably believed that the use or disclosure was necessary to lessen or prevent a serious threat to an individual's life, health or safety, or public health or public safety.

61.35 The recommendations in Chapter 4 are aimed at achieving national consistency in privacy regulation and, in particular, one set of privacy principles applying across the private sector, and the federal, state and territory public sectors. Any legislation establishing the UHI and SEHR schemes should also apply nationally to ensure consistency between the public and private sectors and across all jurisdictions. Finally, and as discussed in detail in Chapter 60, it would be extremely undesirable to have two sets of privacy principles, one set dealing with health information and one set dealing with other personal information. One set of UPPs, amended where necessary by the new *Privacy (Health Information) Regulations* will achieve an appropriate level of regulation and consistency across sectors and jurisdictions.

Recommendation 61–1 If a national Unique Healthcare Identifiers (UHIs) or a national Shared Electronic Health Records (SEHR) scheme goes forward, it should be established under specific enabling legislation. This legislation should address information privacy issues, such as:

(a) the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;

33 Rec 30–6.

(b) the eligibility criteria, rights and requirements for participation in the UHI and SEHR schemes by health consumers and health service providers, including consent requirements;

(c) permitted and prohibited uses and linkages of the personal information held in the systems;

(d) permitted and prohibited uses of UHIs and sanctions in relation to misuse; and

(e) safeguards in relation to the use of UHIs, including providing that it is not necessary to use a UHI in order to access health services.

Medicare and Pharmaceutical Benefits databases

61.36 The Australian Government databases containing personal information collected in connection with claims under the Pharmaceutical Benefits Program and the Medicare Benefits Program are examples of national electronic health records. These databases are subject to specific privacy controls over and above those set out in the *Privacy Act*, including binding guidelines issues by the Privacy Commissioner.

61.37 Section 135AA of the *National Health Act 1953* (Cth)[34] deals specifically with the personal information held in these databases. The section requires the Privacy Commissioner to issue written guidelines covering the storage, use, disclosure and retention of the information.[35] The section applies only to information stored in computer databases—principally those held by Medicare Australia and DOHA—and was introduced to ensure the functional separation of information collected in relation to Medicare claims and information collected in relation to pharmaceutical benefits claims.[36]

61.38 This separation was intended to

> accord with the individual patient's expectation that sensitive health information given in a particular context is used and managed by the recipient in a way that is consistent and in accordance with that context. It gives a practical expression, in the

34 Inserted into the *National Health Act 1953* (Cth) by the *Health Legislation (Pharmaceutical Benefits) Amendment Act 1991* (Cth). In addition, s 27(1)(pa) of the *Privacy Act 1988* (Cth) provides that the issue of guidelines under the *National Health Act* is one of the functions of the Privacy Commissioner.

35 Section 27(1)(pa) of the *Privacy Act 1988* (Cth) provides that one of the functions of the Privacy Commissioner is to issue guidelines under s 135AA of the *National Health Act 1953* (Cth).

36 Commonwealth, *Parliamentary Debates*, House of Representatives, 30 May 1991, 4490 (P Staples—Minister for Aged, Family and Health Services).

> context of information storage systems, to the privacy principle that information should generally only be used for the purpose for which it was collected.[37]

61.39 While the information in the two databases is kept functionally separate, it is possible to disclose the information for research purposes, either with consent from the individuals who are the subject of the information or in accordance with guidelines issued by the National Health and Medical Research Council under s 95 of the *Privacy Act*. The Department of Health Western Australia has noted that:

> Under current legislation and guidelines, it is possible to create linkable MBS and PBS datasets that contain common encrypted identifiers with ethics clearance. The [Data Linkage Unit] has created linkage keys for these datasets and for Residential Aged Care data from the Department of Health and Ageing that enable unidentifiable data to be provided to researchers in approved projects. Research projects are strictly regulated and 're-identification' and unauthorized linkages are forbidden.[38]

61.40 The Privacy Commissioner first issued the *Medicare and Pharmaceutical Benefits Program Privacy Guidelines* in 1993 and they have been revised on a number of occasions.[39] The most recent revision took place between 2004 and 2007 and the revised *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* will come into force on 1 July 2008.[40] The Guidelines are legally binding and any breach is an 'interference with privacy' that may provide the basis for a complaint to the Privacy Commissioner.[41] The Guidelines impose obligations on Australian Government agencies in addition to the Information Privacy Principles (IPPs) in the *Privacy Act* and the secrecy provisions in the *National Health Act 1953* (Cth) and the *Health Insurance Act 1973* (Cth).

61.41 The Guidelines require that claims information collected in connection with the Medicare and Pharmaceutical Benefits Programs be stored in separate databases, and specify the circumstances in which data from the two databases may be linked and retained in linked form.[42] The Guidelines impose standards that are in addition to the requirements imposed by the IPPs. In some instances, the Guidelines set a higher standard of protection for claims information than that required under the *Privacy Act*.

---

37 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997), Commissioner's Note on cl 1.1.

38 Department of Health Western Australia, *Submission PR 139*, 23 January 2006. The use of health information for research is discussed in detail in Ch 58.

39 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997). The guidelines are disallowable instruments. They must be tabled in the Australian Parliament and are then subject to disallowance for a period of 15 sitting days.

40 Office of the Privacy Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs: Issued under Section 135AA of the National Health Act 1953* (2008).

41 *Privacy Act 1988* (Cth) s 13(bb); *National Health Act 1953* (Cth) s 135AB.

42 Office of the Privacy Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs: Issued under Section 135AA of the National Health Act 1953* (2008).

The Guidelines also deal with a number of issues not covered by the IPPs. For example, the Guidelines impose specific obligations in relation to the retention and destruction of claims information. Guideline 9 makes it clear that the Guidelines prevail where they impose more restrictive obligations than the IPPs. The Guidelines, however, cannot permit something that is otherwise prohibited by the IPPs.[43]

61.42 The most recent review of the Guidelines by the Privacy Commissioner[44] was prompted by a number of factors, including: a request from DOHA; suggestions that the personal information covered by the Guidelines could be used more effectively by researchers; and suggestions that community attitudes and expectations regarding the handling of personal information, and in particular sensitive health information, may have changed since the Guidelines were issued.[45] An issues paper[46] was released and 35 submissions were received in the course of the review. A number of open forums were held in late 2004 and a Consultative Group was established to assist the Commissioner in considering the issues raised in the review.

61.43 The major issues canvassed in the course of the review were the:

- separation of claims information collected under the Medicare and Pharmaceutical Benefits programs;
- circumstances in which claims information from each program may be linked;
- periods for which claims information may be retained;
- use of claims information for medical and other research purposes;
- handling by DOHA of claims information that does not identify individuals; and
- application of the Guidelines to agencies other than Medicare Australia and DOHA.[47]

61.44 The Privacy Commissioner's final report was released in August 2006 and included 25 findings.[48] Some of the findings are reflected in the revised Guidelines and

---

43 Office of the Privacy Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs: Explanatory Statement* (2008).

44 K Curtis (Privacy Commissioner), 'Media Statement: 2004 Review of the Medicare and PBS Privacy Guidelines Issued under Section 135AA of the National Health Act 1953' (Press Release, 8 November 2004).

45 Office of the Privacy Commissioner, *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS Claims Information* (2006), 11.

46 Office of the Privacy Commissioner, *Review of the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issues Paper* (2004).

47 Office of the Privacy Commissioner, *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS Claims Information* (2006), 14.

48 Ibid, 8–10.

others indicate the Privacy Commissioner's approach to interpretation of the Guidelines. Significant changes to the Guidelines as a result of the review include the:

- introduction of a new guideline prohibiting any Australian Government agency from combining information obtained from the Medicare Benefits or Pharmaceutical Benefits programs on the one database;

- variation of the period for which linked datasets may be retained by Medicare Australia from a prescribed period (three months) to a principles-based approach whereby the datasets may be retained for as long as is reasonably necessary to fulfil the purpose for which they were created; and

- introduction of a requirement that Medicare Australia report annually to the Privacy Commissioner on how many records from each program are linked, under what authority they are linked, how many of these linked datasets were destroyed in the period (or why they were not destroyed).[49]

61.45 In light of this recent comprehensive review, the ALRC does not consider it necessary to conduct another detailed examination of the Guidelines.

Submissions and consultations

61.46 In IP 31, the ALRC asked whether the role provided for the Privacy Commissioner under s 135AA of the *National Health Act* is an appropriate and effective one.[50] The OPC submitted that the role is appropriate.[51] Other stakeholders were also supportive.[52]

61.47 In contrast, the Department of Human Services stated:

> There is a separate and fundamental question about whether there is still a requirement for section 135AA itself. The information in the Medicare and Pharmaceutical Benefits Scheme claims databases is subject not only to the *Privacy Act* but also to the secrecy provisions of the legislation administered by Medicare Australia. The appropriate application of the privacy principles and secrecy provisions to that information should provide sufficient protection, and as such there is a question about whether there continues to be a need for a separate regime for the handling of the information in those two databases.[53]

---

49 Office of the Privacy Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs: Explanatory Statement* (2008).

50 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006) Question 8–6.

51 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

52 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; W Caelli, *Submission PR 99*, 15 January 2007; A Smith, *Submission PR 79*, 2 January 2007.

53 Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

ALRC's view

61.48 Where personal information is held in major national databases that rely on the use of 'identifiers' such as the Medicare number,[54] there is a role for the Privacy Commissioner to be involved actively, providing extra oversight and developing binding rules in relation to the handling of that information. In these circumstances, the privacy principles and relevant secrecy provisions may not provide sufficient guidance. Importantly, the current *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* vary the application of some of the IPPs, reflecting the special sensitivity attaching, for example, to linkage, comparison or combination of records from the two regulated databases.

61.49 In Chapter 47, the ALRC considers the role of the Privacy Commissioner more generally in issuing non-binding guidelines and binding rules and expresses the view that the power to issue guidance is an important part of regulating a principles-based regime such as the *Privacy Act*. The ALRC expresses the view that where guidelines issued by the Privacy Commissioner are binding they should be renamed 'rules' and recommends that the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* issued under s 135AA of the *National Health Act* should be renamed the *Privacy Rules for the Medicare Benefits and Pharmaceutical Benefits Programs*.[55]

54 Identifiers are discussed in detail in Ch 30.
55 Rec 47–2.

62. The *Privacy Act* and Health Information

Contents

Introduction

62.1 This chapter examines the key definitions in the *Privacy Act 1988* (Cth) relating to the handling of health information—that is, the definitions of 'health information' and 'health service'. The chapter also examines the impact of the Act on the provision of health services and a number of concerns raised in this context, including the issues of consent and capacity. These issues are discussed more generally in Chapters 19 and 70.

62.2 The Information Privacy Principles (IPPs) in the *Privacy Act* do not distinguish between 'personal information', 'sensitive information' and 'health information'. Public sector agencies are required to deal with all personal information, including health information in the same way; that is, in accordance with the IPPs.

62.3 The National Privacy Principles (NPPs), however, provide a separate regime for 'sensitive information', including 'health information', and make specific provision for the handling of health information in some circumstances. This regime applies to private sector organisations, including all organisations that hold health information and provide a health service that might otherwise be exempt from the provisions of the *Privacy Act* under the small business exemption.[1]

62.4 The NPPs require that sensitive information, including health information, be given a higher level of protection than other personal information. For example, sensitive information must be collected with consent, except in a range of specified

1 *Privacy Act 1988* (Cth) s 6D(4)(b). The need for a single set of Unified Privacy Principles (UPPs) applying to both agencies and organisations is discussed in detail in Part D. The small business exemption is discussed in Ch 39.

circumstances.[2] It may be used or disclosed only for the purpose for which it was collected or a directly related secondary purpose—and only so long as the individual would reasonably expect the information to be used in this way.[3] There is also special provision in the NPPs for the:

- collection, use or disclosure of health information for research, or the compilation or analysis of statistics, relevant to public health or public safety;[4]
- collection of health information for the management, funding or monitoring of a health service;[5]
- collection of health information if necessary to provide a health service to the individual and the information is collected as required or authorised by or under law or in accordance with rules relating to professional confidentiality;[6] and
- disclosure of health information to a person who is responsible for the individual, for example, a member of the individual's family, where the individual is physically or legally unable to consent to disclosure.[7]

Definition of 'health information'

62.5 The *Privacy Act* defines 'health information' as follows:

> (a) information or an opinion about:
>
> (i) the health or a disability (at any time) of an individual; or
>
> (ii) an individual's expressed wishes about the future provision of health services to him or her; or
>
> (iii) a health service provided, or to be provided, to an individual;
>
> that is also personal information; or
>
> (b) other personal information collected to provide, or in providing, a health service; or
>
> (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
>
> (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.[8]

---

2 Ibid sch 3, NPP 10.
3 Ibid sch 3, NPP 2.1(a)(i).
4 Ibid sch 3, NPPs 2.1(d), 10.3(a)(i). Research is discussed in detail in Chs 64–66.
5 Ibid sch 3, NPP 10.3(a)(iii). This issue is discussed in Ch 63.
6 Ibid sch 3, NPP 10.2. This issue is discussed in Ch 63.
7 Ibid sch 3, NPPs 2.4–2.6. This issue is discussed in Ch 63.
8 Ibid s 6. Paragraph (d) was added under *Privacy Legislation Amendment Act 2006* (Cth) sch 2, cl 2.

62.6 Paragraph (d) of this definition was added in response to a recommendation by the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC) in *Essentially Yours: The Protection of Human Genetic Information* (ALRC 96).[9] That Report considered the definition of 'health information', as well as the definition of 'sensitive information', and concluded that there were circumstances in which genetic information may not fall within the existing definitions. This might arise where the information is not about health, disability or the provision of a health service—as in the case of parentage or forensic testing—or because it is not about the health or disability of an existing individual—as may sometimes be the case with genetic carrier testing, where the information is primarily about the health of future children.[10]

62.7 The ALRC and AHEC recommended that the definition of 'health information' should be amended to include 'genetic information about an individual in a form which is or could be predictive of the health of the individual or any of his or her genetic relatives'.[11] In September 2006, the *Privacy Legislation Amendment Act 2006* (Cth) was passed. The Act amended the definition of 'health information' in line with the ALRC and AHEC's recommendation.

62.8 The definition of 'health information' in the draft *National Health Privacy Code* includes a similar list of elements to the *Privacy Act* definition. The major difference in the draft Code definition is that it expressly includes information or opinion about 'the physical, mental or psychological health (at any time), of an individual'.[12]

62.9 The definitions of 'health information' in the New South Wales *Health Records and Information Privacy Act 2002*, the Victorian *Health Records Act 2001* and the Northern Territory *Information Act 2002*[13] contain similar elements. The ACT *Health Records (Privacy and Access) Act 1997* defines 'personal health information' more simply, as follows:

> any personal information, whether or not recorded in a health record—
>
> (a) relating to the health, an illness or a disability of the consumer; or
>
> (b) collected by a health provider in relation to the health, an illness or a disability of the consumer.[14]

---

9 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

10 Ibid, [7.75].

11 Ibid, Rec 7–4.

12 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4, cl 1.

13 *Health Records and Information Privacy Act 2002* (NSW) s 6; *Health Records Act 2001* (Vic) s 3; *Information Act 2002* (NT) s 4.

14 *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary.

Issues Paper 31

62.10 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether the definition of 'health information' in the draft *National Health Privacy Code* was appropriate and effective and whether that definition should be adopted into the *Privacy Act*.[15] The ALRC was interested in receiving views on whether adding the terms 'physical, mental or psychological' to the definition of 'health information' would be of benefit.

62.11 In its submission to IP 31, the Department of Health and Ageing (DOHA) expressed support for the current definition in the *Privacy Act.* DOHA noted that the dictionary definition of health includes health of body and mind.[16] The *Macquarie Dictionary* defines 'health' as 'soundness of body; freedom from disease or ailment' or 'the general condition of the body or mind with reference to soundness and vigour'.[17] DOHA was of the view that the words 'physical, mental or psychological' included in the draft *National Health Privacy Code*, were unnecessary.

62.12 The Office of the Privacy Commissioner (OPC) expressed the view that:

> The proposed NHPC expressly includes 'mental and psychological health' as categories of 'health information', though the existing definition of the *Privacy Act* would already appear to comfortably allow for such an interpretation. In the Office's view, a common sense interpretation of health information would include information relating to mental health.[18]

62.13 The NHMRC, however, stated in its submission that:

> The NHMRC is concerned to ensure that the definitions of 'health information' and 'health service' in the *Privacy Act* reflect contemporary and evolving concepts of health and wellbeing.
>
> While many stakeholders would consider that the term 'health' encompasses physical, mental and psychological elements, others draw a distinction between physical 'health' and mental/psychological 'wellbeing'. For clarity, therefore, we support incorporation in the *Privacy Act* of the more expansive definition included in the draft *National Health Privacy Code*.[19]

62.14 A number of other stakeholders also expressed support for the definition in the draft *National Health Privacy Code*.[20]

---

15 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–7.
16 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.
17 *Macquarie Dictionary* (online ed, 2007).
18 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
19 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
20 Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

Discussion Paper proposal

62.15 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72),[21] the ALRC noted that the dictionary definition of the term 'health' is broad enough to cover mental and psychological health as well as physical health. The ALRC noted, however, the NHMRC's comment that a distinction is sometimes drawn between physical health and mental or psychological wellbeing. The ALRC expressed the view that the *Privacy Act* should be clear on this point, especially given the sensitivity of personal information about mental or psychological health. The ALRC proposed, therefore, that the definition of 'health information' in the *Privacy Act* be amended to make express reference to information or an opinion about the *physical, mental or psychological* health or disability of an individual.[22]

Submissions and consultations

62.16 A significant number of stakeholders, including the NHMRC, the Department of Human Services, Medicare Australia, the Victorian Office of the Health Services Commissioner, the Australian Privacy Foundation and the Public Interest Advocacy Centre (PIAC), expressed support for this proposal.[23]

62.17 On the other hand, the New South Wales Department of Health was of the view that it was unnecessary to include the term 'psychological' in the definition as psychological health is subsumed in the broader term 'mental health'. The Department noted that the *Health Records and Information Privacy Act 2002* (NSW) refers to 'physical or mental health'.[24]

62.18 Some stakeholders expressed the view that the addition of the words 'physical, mental or psychological' did not add anything and that the existing definition of 'health information' should be retained.[25] The OPC agreed, noting that the proposal was to 'explicitly incorporate types of health information that are already recognised implicitly by the current definition of health information'. The OPC expressed concern that the proposed amendment might narrow the definition and reduce its flexibility by introducing a list of the types of health information covered by the Act. In addition, the

---

21 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007).

22 Ibid, Proposal 57–1.

23 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007; Pharmacy Guild of Australia, *Submission PR 433*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

24 *Health Records and Information Privacy Act 2002* (NSW) s 6(a)(i).

25 Confidential, *Submission PR 570*, 13 February 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

OPC was concerned that amending the definition of health information in this way would introduce a level of inconsistency between the definition of 'health information' in the *Privacy Act* and the definition of a 'health service'.[26]

ALRC's view

62.19 The ALRC notes the strong support among stakeholders for including a reference to mental and psychological health in the definition of 'health information'. The ALRC is concerned that the term 'health' is sometimes interpreted to mean 'physical health'. Including the terms 'physical, mental or psychological' will not narrow the definition of health information, particularly as the existing definition includes 'other personal information collected to provide, or in providing, a health service'. Rather, the addition of the terms will make it clear that 'health information' is not intended to be restricted to personal information about an individual's physical health.

62.20 The ALRC also notes that, while there is overlap between the terms mental health and psychological health, there are also distinctions drawn between these two areas. For example, the Australian Psychological Society draws a distinction between the work of psychologists, who 'help mentally healthy people find ways of functioning better', and psychiatrists, who 'mainly treat people with mental illness, such as schizophrenia'.[27] It is important, therefore, to include both mental and psychological health in the definition. The *Privacy Act* should be amended to make clear that 'health information' includes information in relation to physical, mental or psychological health. It is preferable to clarify the point by amendment, rather than wait for the issue to arise in the context of a complaint.

Recommendation 62–1 The definition of 'health information' in the *Privacy Act* should be amended to make express reference to the *physical, mental or psychological* health or disability of an individual.

Definition of 'health service'

62.21 Another definition that is central to the way health information is handled under the *Privacy Act* is the definition of a 'health service'. The term 'health service' is used in the *Privacy Act* in a range of circumstances. These include: as part of the definition of 'health information'; as a limitation on the scope of the small business exemption—small businesses that hold health information and provide a health service are not covered by the small business exemption; and as a 'permitted purpose' under Part VIA dealing with declared emergencies and disasters.

---

26 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

27 Australian Psychological Society, *Psychologists and Psychiatrists* <www.psychology.org.au/community/about/> at 14 April 2008.

62.22 In addition, the term is used in several provisions that provide for the use of health information in circumstances that would normally breach the IPPs or NPPs. For example, under NPP 2.1(ea), the genetic information of one individual, collected in the course of providing a health service, may be disclosed in certain circumstances to a genetic relative of that individual without consent.[28] A health service provider may disclose personal information to a person 'responsible for the individual' where the individual is physically or legally incapable of giving consent to the disclosure or physically cannot communicate consent.[29] Finally, an organisation may collect health information without consent where it is necessary to provide a health service to the individual[30] or where necessary for the management, funding and monitoring of a health service.[31]

62.23 The *Privacy Act* defines a 'health service' as follows:

> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
>
> (i) to assess, record, maintain or improve the individual's health; or
>
> (ii) to diagnose the individual's illness or disability; or
>
> (iii) to treat the individual's illness or disability or suspected illness or disability; or
>
> (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.[32]

62.24 The definition of 'health service' in the draft *National Health Privacy Code* has a number of differences, including express references to injuries, disability support services, palliative care services, and aged care services. The draft Code definition is as follows:

> 'health service' means—
>
> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual service provider or the organisation performing it—
>
> (i) to assess, maintain or improve the individual's health; or
>
> (ii) to diagnose the individual's illness, injury or disability; or
>
> (iii) to treat the individual's illness, injury or disability or suspected illness, injury or disability; or
>
> (b) a disability service, palliative care service or aged care service; or

---

28 NPP 2.1(ea) is discussed further in Ch 63.
29 *Privacy Act 1988* (Cth) sch 3, NPP 2.4.
30 Ibid sch 3, NPP 10.2.
31 Ibid sch 3, NPP 10.3.
32 Ibid s 6.

> (c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist—
>
> but does not include a health service, or a class of health service, that is prescribed as an exempt health service or to the extent that it is prescribed as an exempt health service.

62.25 The definition in the Victorian *Health Records Act* is very similar to that in the draft Code.[33] The definitions in the ACT health records legislation and the Northern Territory *Information Act* have many of the same elements.[34] The New South Wales legislation, however, takes a different approach, setting out a non-exhaustive list of the services covered—such as medical, hospital and nursing services, dental services and mental health services—rather than describing them in more general terms.[35]

Issues Paper 31

62.26 In IP 31, the ALRC asked whether the definition of 'health service' in the draft *National Health Privacy Code* was appropriate and effective and whether that definition should be adopted into the *Privacy Act*.[36]

62.27 There was some support expressed in submissions to IP 31 for the definition of 'health service' in the draft *National Health Privacy Code*.[37] The NHMRC stated that:

> We are aware also that there is some debate in the Aged Care sector about whether residential aged care is a health service or a social/accommodation service. We support, therefore, the inclusion of a more expansive definition of 'health service' in the *Privacy Act*, incorporating reference to 'disability services', 'palliative care services', 'aged care services' and 'injury' explicitly, thereby avoiding any potential uncertainty.[38]

62.28 A number of other stakeholders agreed that the definition should be amended to cover the services that people with a disability, and those in palliative and residential aged care might use. These services provide care, supervision and assistance with daily life, rather than treatment.[39]

62.29 The Office of the Health Services Commissioner in Victoria expressed the view that:

---

33 *Health Records Act 2001* (Vic) s 3.

34 *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary; *Information Act 2002* (NT) s 4.

35 *Health Records and Information Privacy Act 2002* (NSW) s 4.

36 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–7.

37 Health and Community Services Complaints Commission (South Australia), *Submission PR 207*, 23 February 2007; Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

38 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

39 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007; Australian Institute of Health and Welfare, *Submission PR 170*, 5 February 2007.

> Organisations providing a broad range of services intended to benefit the health and well-being of individuals, should be subject to the same privacy standards. As an example, HSC has received health privacy complaints concerning alternative therapists, which are included in the definition of health service under the *Health Records Act* and the *National Code*. The problem with the New South Wales approach is that a non-exhaustive definition that focuses on conventional medical and health services may be interpreted to exclude some alternative therapists, which might leave the public vulnerable.[40]

62.30 The OPC raised a number of concerns with the definition of 'health service' in the draft *National Health Privacy Code*, including the fact that the definition does not refer to 'recording' an individual's health information. The draft Code definition also relies exclusively on the understanding of the health service provider as to whether a particular activity is intended or claimed to have health benefits. In contrast, the *Privacy Act* allows this to be judged from the perspective of the health service provider or the health consumer. The OPC did, however, express support for one element of the definition:

> The Office also notes that the word 'injury' is added in addition to illness and disability in (a)(ii) and (iii) of the proposed NHPC definition. The nature of an injury appears to be distinct from the inherent properties of an illness or a disability, and as such, the inclusion of this word may increase the clarity of the definition.[41]

Discussion Paper proposal

62.31 In DP 72, the ALRC proposed that the definition of 'health service' in the *Privacy Act* should be extended to cover disability services, palliative care services and aged care services. These services do not fall comfortably within the existing definition of 'health services'. They are, however, aimed at providing physical, mental and psychological care and support to individuals and often require the collection, use and disclosure of significant amounts of health information. The ALRC also expressed the view that an 'injury', as distinct from an 'illness' or a 'disability', should be referred to expressly in the definition of 'health service'.

Submissions and consultations

62.32 A number of stakeholders expressed support for expanding the definition of 'health service' to include injuries and disability services, palliative care services and aged care services.[42] The OPC suggested, however, qualifying the references to

---

40 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

41 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

42 Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Medical Association, *Submission PR 524*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Pharmacy Guild of Australia, *Submission PR 433*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007.

disability, aged care and palliative care services to exclude services unrelated to health such as advocacy services.[43]

62.33 The Centre for Law and Genetics stated that:

> We strongly support the proposed amendments to the definition of health service to ensure that complementary therapies are included. There has been a massive increase in the development, marketing and advertising of complementary 'health' products and services. These service providers should be governed by regulations no less prescriptive than those applying to the traditional health service agencies and organisations.[44]

62.34 Other stakeholders agreed that the definition should extend to complementary and alternative therapies and to 'wellness' services; for example, those related to pregnancy and weight loss.[45] The NHMRC suggested that cosmetic surgical procedures would not be covered by the existing definition and that the definition of 'health service' be amended to refer to the 'prevention' of illness:

> We believe that prevention of illness (for example through immunisation) differs from maintenance of health, which we consider indicates an active intervention once a risk factor or disease has been identified (for example, through the supply or prescription of medications to control an individual's blood cholesterol or blood pressure).[46]

62.35 The NHMRC also noted that a number of organisations offer genetic or other testing but do not claim to use this information to assess, predict, maintain or improve an individual's health. Such tests are offered, for example, by providers of skin care and dietary products.

62.36 The NHMRC also discussed the case of Australian Biologics Testing Services. The Australian Competition and Consumer Commission (ACCC) instituted proceedings in the Federal Court of Australia against Australian Biologics alleging that representations made in its brochures and on its website were false, misleading, and deceptive. The representations included that thermography tests offered by Australian Biologics could be used for diagnostic purposes in the cardiac field. The ACCC alleged that the representations were not supported by scientific or medical testing.[47] The case was settled by consent on the basis that:

> Australian Biologics agreed that the tests it offers are not diagnostic and the results of such tests are not indicative of a specific medical condition and undertook not to make a number of claims relating to the utility of its services for the diagnosis of specific medical conditions.[48]

---

43 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

44 Centre for Law and Genetics, *Submission PR 497*, 20 December 2007.

45 New South Wales Government Department of Health, *Submission PR 458*, 11 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

46 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

47 Australian Competition and Consumer Commission, 'ACCC Settles Proceedings Against Australian Biologics' (Press Release, 15 July 2004).

48 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

62.37 A number of stakeholders were of the view that simply 'recording' health information should not be sufficient to bring an agency or organisation within the definition of a health service provider.[49] On the other hand, the OPC was of the view that the term 'record' should remain in the definition:

> Nevertheless, the Office notes the potential ambiguity between organisations which record an individual's *health* in the course of providing a health service, and entities which may record or document *health information* in ways that would not ordinarily be considered to be health service provision. The second category may include the recording of health information by health insurance companies, employers and others.[50]

62.38 The Victorian Office of the Health Services Commissioner stated that:

> HSC believes the term 'record' is not necessary in the definition of health service, as it does not add anything that is not already covered by the other definitions. The example given at paragraph 57.26 is of health monitoring, which involves recording someone's blood pressure, height and weight with no further action taken unless a change occurs. Such an organisation recording this information would be doing so to assess or improve an individual's health or to diagnose or treat a condition, and would therefore be covered by the other definitions.[51]

62.39 Certain other stakeholders asked whether the provision of health insurance came within the definition of a health service.[52] Medicare Australia stated that:

> Medicare Australia also receives many thousands of requests from insurance companies that seek information about pre-existing illnesses while processing claims. We take great care to ensure that the claimants provide informed consent in these cases. It is very important that these requests should not be seen as 'collection where it is necessary to provide a health service'.[53]

ALRC's view

62.40 The ALRC notes that the term 'health service' is used in the *Privacy Act* as part of the definition of 'health information', and to allow more permissive collection, use and disclosure of health information in the health services context than would normally be allowed under the NPPs. For example, under NPP 10.2, a doctor may collect health information about an individual without consent where that individual is unconscious, or too ill to provide consent, and the collection is related to providing care and treatment for the individual.

62.41 It is important to ensure that the definition of 'health service' is appropriately limited to the provision of services intended, for example, to assess or improve the

---

49 See, eg, Confidential, *Submission PR 570*, 13 February 2008.
50 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
51 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.
52 Confidential, *Submission PR 519*, 21 December 2007.
53 Medicare Australia, *Submission PR 534*, 21 December 2007.

individual's health and does not extend to activities such as providing health insurance. It would not be appropriate for the more permissive provisions on collection, use and disclosure of health information to occur in the health insurance context. For this reason, the ALRC recommends that 'recording' an individual's health should be removed from the definition of 'health service'. The term is unnecessary and that it may lead to undesirable outcomes.

62.42 The definition should continue to allow the assessment of the service to be made by the individual or the service provider. The ALRC did not receive any submissions indicating problems with the existing provision.

62.43 The ALRC also recommends that the definition of 'health service' be amended to include activities that:

- 'predict' the individual's physical, mental or psychological health or status, in order to accommodate some forms of genetic testing;

- 'prevent' illness, injury or disability in order to cover, for example, services to assist with diet and weight loss and immunisations; and

- assess or predict the individual's physical, mental or psychological 'status'. This change is intended to capture a range of things such as genetic or other testing that is not primarily concerned with the health or disability of an existing individual—as may sometimes be the case with genetic carrier testing, where the information is primarily about the health of any possible future children.

62.44 The ALRC also recommends the inclusion of surgical or related services to capture cosmetic procedures, and has taken up the OPC's suggestion that disability, palliative care or aged care services should be limited to health-related services. Finally, the definition should be amended to include 'injuries' as well as 'illness' and 'disability'.

Recommendation 62–2 The *Privacy Act* should be amended to define a 'health service' as:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

  (i) assess, predict, maintain or improve the individual's physical, mental or psychological health or status;

  (ii) diagnose the individual's illness, injury or disability; or

(iii) prevent or treat the individual's illness, injury or disability or suspected illness, injury or disability;

(b) a health-related disability, palliative care or aged care service;

(c) a surgical or related service; or

(d) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Agencies and organisations

62.45 Broadly speaking, Australian Government agencies are required to handle health information in accordance with the IPPs. Private sector organisations are required to handle health information in accordance with the NPPs. There are a number of significant exemptions in the *Privacy Act*, however, that mean that some agencies and organisations holding health information may not be subject to the Act in relation to that information.[54]

62.46 Perhaps the most significant exemption in the context of health information is for small business operators. Section 6D of the *Privacy Act* defines a small business as one that has an annual turnover of $3 million or less in the previous financial year.[55] Some small businesses operators that pose a higher risk to privacy have been brought back into the regime. In particular, small businesses are required to comply with the NPPs if, among other things, they:

- provide a health service and hold health information, except where the information is held in an employee record;
- disclose personal information for a benefit, service or advantage; or
- provide a benefit, service or advantage to collect personal information.[56]

62.47 Small businesses that hold health information and provide a health service, therefore, are bound by the NPPs. This leaves open the possibility, however, that small

54 Exemptions are discussed in detail in Part E.

55 Ch 39 examines the small business exemption in detail.

56 *Privacy Act 1988* (Cth) s 6D(4). Note that s 6D(7)–(8) of the *Privacy Act* provides that small businesses trading in personal information may not be required to comply with the NPPs if they have the consent of the individuals concerned or if the collection or disclosure of personal information is required or authorised by law.

businesses that hold health information but do not provide health services, do not pay to collect the information and are not paid to disclose the information—for example, health data registers that store health information for research purposes—may not be required to comply with the Act.

62.48 This possibility was considered in ALRC 96 in relation to genetic information. The ALRC and AHEC concluded that: small businesses that hold genetic information should be subject to the provisions of the *Privacy Act*, whether or not they provide a health service; and there was sufficient doubt about the coverage of *Privacy Act* to justify amending the Act to make it clear that all small businesses that hold genetic information are subject to its provisions.[57]

62.49 The Australian Government did not support this recommendation. The Government considered that the existing provisions provided sufficient protection for the privacy of genetic information held by small businesses, while at the same time ensuring that small businesses were not burdened unfairly by the costs of complying with privacy legislation.[58]

62.50 The draft *National Health Privacy Code*, by way of contrast, is expressed to apply to 'every organisation that is a health service provider or collects, holds or uses health information'.[59] The Victorian *Health Records Act* also applies to organisations that are health service providers or collect, hold or use health information.[60] The Act does not exempt small business operators. On the other hand, the New South Wales *Health Records and Information Privacy Act* exempts small business operators by reference to the *Privacy Act.*[61]

62.51 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act.[62]

Submissions and consultations

62.52 DOHA noted in its submission that:

> It is considered that given its characteristics and sensitivities, individuals need reassurance that their health information will be handled appropriately by whoever holds it. Any misuse will heighten concerns about disclosing this kind of information,

---

57 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–7.

58 Australian Government Attorney-General's Department, *Government Response to Australian Law Reform Commission and Australian Health Ethics Committee Report: Essentially Yours: The Protection of Human Genetic Information in Australia* (2005) <www.ag.gov.au> at 24 April 2008, 8.

59 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 2 div 1 cl 1.

60 *Health Records Act 2001* (Vic) s 11.

61 *Health Records and Information Privacy Act 2002* (NSW) s 4.

62 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–8.

> and unwillingness to disclose this information in a healthcare setting could result in detriment to the individual concerned or to the community as a whole.[63]

62.53 DOHA expressed the view that the handling of health information should be subject to appropriate privacy regulation across both the public and private sectors, although noting the need for some exemptions for agencies and organisations, such as the courts. Other stakeholders agreed that appropriate privacy regulation should apply in both the public and private sectors and regardless of the size of the business involved.[64]

62.54 In its submission, the NHMRC stated that:

> The NHMRC cannot identify any relevant policy rationale for excluding the majority of small businesses from compliance with the *Privacy Act*. We consider that it is vitally important that the protections currently provided for health information apply to *all* agencies and organisations that handle health information (including genetic information) and to all agencies and organisations that handle genetic information that is not health information.[65]

ALRC's view

62.55 Part E examines the policy basis for each of the exemptions from the *Privacy Act* and makes recommendations for change where necessary. In Chapter 39, the ALRC recommends the removal from the *Privacy Act* of the small business exemption. For the reasons discussed in that chapter, the ALRC is not convinced that an exemption for small business is either necessary or justifiable. The fact that comparable overseas jurisdictions—including the United Kingdom, Canada and New Zealand—do not have an exemption for small business is a relevant consideration.

62.56 In Chapter 40, the ALRC also recommends the removal from the Act of the employee records exemption. This will extend for the first time privacy protections to health information held in private sector employee records.

62.57 The recommendations in Parts D and E, once implemented, will ensure that personal information—and, in particular, health information—will receive appropriate

---

63 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

64 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Royal Women's Hospital Melbourne, *Submission PR 108*, 15 January 2007; K Pospisek, *Submission PR 104*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006; A Smith, *Submission PR 79*, 2 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

65 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

protection in the Australian Government public sector and the private sector. The recommendations in Chapter 3, aimed at achieving national consistency, will extend this protection into state and territory public sectors. These n combination will mean that the handling of health information is regulated consistently and appropriately throughout Australia.

Provision of health services

62.58 The following section deals with the impact of the *Privacy Act* on the provision of health services to health consumers. It was suggested in consultations that the *Privacy Act* impeded the provision of health services to consumers, for example, by interfering with the appropriate sharing of an individual's health information between members of the team of health professionals treating the individual.[66] This may be a result of problems with the *Privacy Act*, which are discussed in Chapter 63 in relation to particular privacy principles, or it may be for other reasons. For example, there may be a chilling effect on the sharing of information based on a misunderstanding of, or an overly cautious approach to, the Act or the privacy principles.

62.59 In its submission to the Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act* (the OPC Review),[67] the NHMRC stated that:

> The NHMRC considers that the application and/or interpretation of the *Privacy Act* is impairing the quality, effectiveness and timeliness of management of health information. In their efforts to ensure compliance with the law, health care professionals and administrators are experiencing considerable difficulty in developing and implementing practical policies that do not 'over-interpret' their obligations and do not impair the legitimate flow of information between providers for patient care purposes.
>
> The NHMRC also considers that the overall public interest and the interests of the majority of individual patients are served by the efficient transfer of all necessary clinical information between health care providers for the purposes of the current care of an individual patient. There is, in fact, considerable potential for individual harm as a result of a privacy regime which results in individual health care providers being uncertain about their legal obligations, afraid of breaking the law by transferring health information without explicit consent, and implementing ineffective and inefficient procedures in their efforts to comply with the law.[68]

66 NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006.

67 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005).

68 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

62.60 The OPC Review recommended the development of further guidance in relation to the use and disclosure of health information in the health services context under the NPPs.[69]

Submissions and consultations

62.61 In its submission to the Inquiry, DOHA stated that:

> It is not possible to point to specific evidence of incidents where the present regulatory environment for health information has impeded the provision of health service delivery. Anecdotally, in handling enquiries on privacy matters Departmental officers are aware of instances where callers have complained about a request for information being refused 'because of the *Privacy Act*'. In discussions with private medical practitioners, frustration has been expressed about not being able to easily obtain information from a public hospital about a recent admission of one of their patients for the purpose of treatment. These kinds of responses and perceptions often result from a misunderstanding of the privacy regulation, something that is not helped by the inconsistencies, complexities and confusion that results from the present regulatory environment.[70]

62.62 This is consistent with comments in other submissions that indicated that the problem is not the content of the privacy principles themselves, but rather a lack of understanding of relevant legislation and principles.[71] The Western Australian Department of Health also suggested that part of the problem lies in changing clinical practice that now involves multiple health service providers from a greater range of institutions in the treatment of one individual. The Department noted the need for communication and education to manage this transition.[72]

62.63 The NHMRC expressed the view that the principles could be made clearer:

> The NHMRC has significant anecdotal evidence and survey responses indicating that disclosure of health information for the purposes of current treatment is being impeded by the privacy regulatory regime. We consider that disclosure of relevant health information for current treatment purposes should be permitted provided there is no indication to the disclosing organisation that such disclosure is or would be unacceptable to the patient; and there are no other circumstances which could reasonably be expected to alert the disclosing organisation that the patient would object to disclosure. We consider that this issue is of sufficient significance to warrant recognition, through a binding determination, legislative or regulatory change, of the circumstances in which disclosure can be made for the purposes of ongoing clinical care.[73]

---

69 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 77, 78.

70 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

71 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; A Smith, *Submission PR 79*, 2 January 2007.

72 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

73 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

62.64 The OPC, however, expressed the view that the NPPs are consistent with best practice and professional ethical standards in the health services context. The OPC suggested that the major impediments to appropriate information flow between health service providers was uncertainty created by regulatory complexity and overlapping and inconsistent legislation regulating the handling of health information in different jurisdictions.[74]

62.65 The Victorian Office of the Health Services Commissioner was of the view that the Health Privacy Principles (HPPs) in the *Health Records Act* were based on good standards of health service delivery and did not cause problems of the type discussed above. The Office suggested that the problem arose from a different source:

> As a result of the introduction of privacy legislation, individuals who believe their privacy has been breached have somewhere to complain, and this makes some health providers more cautious in their dealings with individuals. Some health service providers have interpreted privacy to mean secrecy. The solution is training, resources and support.[75]

ALRC's view

62.66 While there was some evidence in submissions and consultations that the regulation of health information in Australia is causing problems for health service providers, there was very little evidence that the problem lies with the IPPs or NPPs. The problems identified included confusion caused by regulatory complexity and a lack of understanding of some of the principles and how they might apply in the health services context. The recommendations in Chapter 3, aimed at achieving national consistency in privacy regulation, in combination with the recommendation for one set of Unified Privacy Principles (UPPs)[76] and a rationalisation of the exceptions and exemptions in the *Privacy Act*,[77] will go a long way towards resolving the uncertainty and confusion caused by the existing regime.

62.67 As discussed in Chapter 4, a principles-based privacy regime focuses on high-level, broadly stated principles rather than detailed, prescriptive rules. This is intended to shift the regulatory focus from process to outcomes. Principles-based regulation facilitates regulatory flexibility through a statement of general principles that can be applied to new and changing situations. This is considered entirely appropriate and workable in the health services context.

62.68 The model UPPs provide that health information generally must be collected with consent, although that consent may be express or implied. Health information may be used or disclosed for the purpose for which it was collected and any other directly related purpose, within the reasonable expectations of the individual health consumer.

---

74 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
75 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.
76 Recommendation 18–2.
77 As recommended in Part E.

These principles provide extensive scope for exchange of information among members of treatment teams, while encouraging good communication with health consumers about the collection, use and disclosure of their health information. They do not require written consent from the health consumer for every collection, use or disclosure, nor do they prevent the sharing of health information among the members of a team of health service providers treating a health consumer. There was no evidence provided to the Inquiry that these basic principles were inappropriate or unworkable, in practice.

62.69 In addition, there are a number of exceptions to the principles that, while applying broadly to personal information, are relevant to the handling of health information in the health services context. These include the exceptions in:

- the 'Collection' principle, which allows the collection of sensitive information, including health information, without consent where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information relates is incapable of giving consent; and

- the 'Use and Disclosure' principle, which allows the use or disclosure of personal information, including health information, if the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety or to public health or public safety.

62.70 Finally, there are a number of principles and exceptions that apply only to health information. In Chapter 60, the ALRC recommends that these principles and exceptions should sit in the new *Privacy (Health Information) Regulations*.[78] Each of these additions to the model UPPs is considered in Chapter 63.

62.71 The OPC Review recommended the development of further guidance in relation to the use and disclosure of health information in the health services context.[79] The ALRC supports this approach and notes that the OPC has issued a number of new information sheets including Information Sheet 25: *Sharing Health Information to Provide a Health Service*.[80] In light of the comments from stakeholders noted above, it seems clear that there is a need for guidance and training for health service providers to ensure a better understanding of the intent and application of principles-based regulation and the privacy principles. In addition, this issue may require further attention from providers of education and training in the health services context. The

78 Rec 60–1.

79 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 77, 78.

80 Office of the Privacy Commissioner, *Sharing Health Information to Provide a Health Service*, Information Sheet 25 (2008).

ALRC notes, however, that in a principles-based regime there always will be a need for the exercise of judgment and discretion by agencies and organisations handling health information.

Consent

62.72 Consent is a central concept in the *Privacy Act*—as it is in health ethics—and is of particular importance in dealing with health information because of the sensitive nature of that information. Consent provisions allow individual health consumers a measure of control over the collection, use and disclosure of their health information. This contributes to an environment in which the autonomy and dignity of the individual are respected, and supports the public interest in health consumers seeking advice and assistance from health service providers when needed, with the assurance that they will be able to maintain appropriate control of their personal information. It is important to note in the context of the *Privacy Act* that the issue under consideration is consent to the handling of health information and not consent to medical treatment.

62.73 The role of consent in the privacy regime generally, including issues such as the definition of consent and the use of 'bundled consent', is considered in detail in Chapter 19. In this chapter the ALRC will consider the role of consent in dealing with health information.

62.74 The OPC *Guidelines on Privacy in the Private Health Sector* (OPC Guidelines) state that the key elements of consent require that:

- it must be provided voluntarily;
- the individual must be adequately informed; and
- the individual must have the capacity to understand and communicate his or her consent.[81]

Consent in the IPPs and the NPPs

62.75 In general terms, both the IPPs and the NPPs attempt to align consent requirements with what reasonable health consumers would expect in relation to the handling of their health information.

62.76 Consent is generally required when collecting health information under the NPPs, subject to a number of specific exceptions.[82] Consent is not required, however, when collecting health information under the IPPs.[83] Consent is not required for use

---

81 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A5.2.
82 *Privacy Act 1988* (Cth) sch 3, NPP 10.1.
83 Ibid s 14.

under the NPPs or the IPPs if health information is used for the purpose for which it was collected or any other directly related purpose and, in the case of the NPPs, individuals would reasonably expect the organisation to use health information in that way.[84]

62.77 Consent is not required for disclosure under the IPPs if the individual was reasonably likely to have been aware that such disclosures are usually made.[85] Consent is not required for disclosure under the NPPs if the information is disclosed for the purpose for which it was collected or a directly related purpose and individuals would reasonably expect the organisation to disclose health information in that way.[86]

62.78 There are a number of exceptions to these general rules. For example, health information may be used without consent under both the IPPs and the NPPs where the use is:

- necessary to lessen or prevent a serious and imminent threat to an individual's life or health;[87]
- required or authorised by law;[88] or
- reasonably necessary to enforce the criminal law.[89]

62.79 In addition, the Act allows health information to be used without consent for research in some circumstances, with the approval of a Human Research Ethics Committee (HREC). This regime is discussed in detail in Chapters 64–66.

Express and implied consent

62.80 'Consent' is defined in the *Privacy Act* as 'express or implied consent'.[90] Express consent 'refers to consent that is clearly and unmistakably stated'.[91] Consent may be stated orally, in writing, electronically or in any other form, so long as it is clearly communicated. Implied consent also requires communication and understanding between health service providers and health consumers. The OPC has stated that:

---

84 Ibid s 14, IPP 10.1; sch 3, NPP 2.1.
85 Ibid s 14, IPP 11.1.
86 Ibid sch 3, NPP 2.1.
87 Ibid s 14, IPP 10.1(b); sch 3, NPP 2.1(e).
88 Ibid s 14, IPP 10.1(c); sch 3, NPP 2.1(g).
89 Ibid s 14, IPP 10.1(d); sch 3, NPP 2.1(h).
90 Ibid s 6.
91 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A5.3.

> If the discussion has provided the individual with an understanding about how their health information may be used, then it would be reasonable for the health service provider to rely on implied consent.[92]

Specific and general consent

62.81 Consent runs along a spectrum from the very specific to the very general. In some cases, consent is sought to a wide range of uses and disclosures of personal information without giving individuals an opportunity to distinguish between those uses and disclosures to which they consent and those to which they do not. This is a particular problem where some of the uses and disclosures bundled together do not relate to the primary purpose of collection. This is referred to as 'bundled consent' and is discussed in Chapter 19.

62.82 In relation to sensitive information, such as health information, it may be reasonable to seek consent to a range of things at the same time—for example, collection into a health record maintained by the health service provider that will be retained for some period into the future; disclosure to, and use by, a pathology laboratory for testing purposes; and disclosure to a medical specialist for expert advice. Consent, however, should not be so general as to undermine the requirements that it be voluntary and adequately informed.

Capacity

62.83 Significant issues arise when individuals do not have the capacity to understand and communicate their consent to the way in which their health information is handled. For example, an adult's decision-making capacity may be impaired temporarily or permanently by injury, illness or disability. This issue is discussed in detail in Chapter 70. Children and young people may have limited capacity to understand and consent. This issue is discussed in Chapters 67–69.

62.84 The draft *National Health Privacy Code* provides detailed provisions relating to the powers of an 'authorised representative'. These provisions include powers to consent to collection, use and disclosure of health information on behalf of an individual who is incapable of giving consent, as well as powers to access and correct health information.[93]

62.85 In IP 31, the ALRC asked whether the *Privacy Act* provides an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent.[94] The ALRC also asked whether there

---

92 Ibid, Guideline A5.3.

93 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4 cl 4.

94 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–11.

are any other issues relating to consent to deal with health information in the health services context that the ALRC should consider.[95]

Submissions and consultations

62.86 In its submission, DOHA stated that:

> Where the individual lacks capacity, it should be permissible for a person who is authorised under general law to make decisions on behalf of the individual, such as a parent, legal guardian or a person with an enduring power of attorney, to give consent, or to exercise rights of access or correction.[96]

62.87 A number of stakeholders expressed the view that detailed guidance was required in this area.[97] There was some support for the approach adopted in the draft *National Health Privacy Code*.[98] The National E-Health Transition Authority (NEHTA) commented, however, that although the draft Code included provision for an 'authorised representative' to make decisions on behalf of an individual, the Code did not allow for less formal arrangements. NEHTA's view was that it was important to allow sufficient flexibility for alternative decision making in the health services context.[99]

ALRC's view

62.88 Chapter 19 discusses in detail the concept of consent, including what amounts to valid consent and the problem of 'bundled consent'. In that chapter the ALRC recommends that the OPC develop and publish guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act* in specific contexts. This would include the health services context and reliance on express and implied consent. The ALRC also recommends that the guidance should address when it is or is not appropriate to use the mechanism of 'bundled consent'.[100]

62.89 The ALRC does not recommend adopting the 'authorised representative' mechanism. Instead, in Chapter 70, the ALRC makes a range of recommendations aimed at facilitating a flexible approach to the involvement of third parties in decision making on behalf of other individuals. These recommendations include the adoption of the concept of a 'nominee'. A nominee, appointed by the individual, may act on behalf

---

95 Ibid, Question 8–12.
96 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.
97 See, eg, Australian Nursing Federation, *Submission PR 205*, 22 February 2007.
98 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
99 National E-health Transition Authority, *Submission PR 145*, 29 January 2007.
100 Rec 19–1.

of the individual in dealing with an agency or organisation that has established arrangements to recognise and verify the nominee. The ALRC recommends that nominees should be under an obligation to act in the best interests of the individual.[101]

62.90 'Nominee' arrangements are based on consent and are intended to be less formal than arrangements such as an enduring power of attorney or a guardianship order. Formal, legal appointments will be required, however, where the individual does not have capacity to appoint a nominee. The ALRC recommends that the OPC develop and publish guidance on dealing with third party representatives and on recognising and verifying substitute decision makers authorised by a federal, state or territory law.[102] The ALRC also recommends that agencies and organisations that regularly handle the personal information of individuals with impaired decision-making capacity should ensure that relevant staff are adequately trained in relation to issues concerning capacity, and in recognising and verifying the authority of third party representatives.[103]

62.91 These recommended provisions, in combination with the model UPPs, will provide an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent. In everyday situations, nominee and other third party representative arrangements may operate. In emergency situations, the 'Collection' principle—which allows the collection of health information without consent where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual—and the 'Use and Disclosure' principle—which allows the use or disclosure of health information where necessary to lessen or prevent a serious threat to an individual's life, health or safety or to public health or public safety—will operate.

101 Rec 70–1.
102 Rec 70–3.
103 Rec 70–4.

63. Privacy (Health Information) Regulations

Contents

Introduction

63.1 In this chapter the ALRC considers those elements of the privacy principles that deal specifically with the handling of health information. As discussed in Chapter 60, the ALRC's view is that these elements should be set out in new *Privacy (Health Information) Regulations*.[1] This approach is intended to ensure that the Unified Privacy Principles (UPPs) remain as brief, general and accessible as possible for those agencies and organisations that do not handle health information. For those agencies and organisations that do handle health information, however, the ALRC recommends that the Office of the Privacy Commissioner (OPC) publish a document setting out the UPPs as amended by the new *Privacy (Health Information) Regulations*. This document will provide a complete set of privacy principles covering health information, as well as other personal information.[2]

63.2 The *Privacy Act* and, in particular, the National Privacy Principles (NPPs) make specific provision for handling health information in a range of circumstances. Each of these provisions is discussed below, including: the collection of family medical history information; the disclosure of health information to a person who is 'responsible' for an individual, where the individual is physically or legally incapable of giving consent; and the disclosure of genetic information to genetic relatives. The chapter also

1 Rec 60–1.
2 Rec 60–2.

considers a number of principles drawn from the draft *National Health Privacy Code*, and recommends that they be included in the *Privacy (Health Information) Regulations*. These include principles relating to the transfer of health information from one health service provider to another when a health consumer changes practices,[3] and the compulsory use of intermediaries where a health service provider has refused to provide a health consumer with access to his or her health information.[4]

Collection of health information

Collection of family medical history information by health service providers

63.3 NPP 10.1 provides that, subject to a number of exceptions, an organisation must not collect sensitive information without consent. This requirement is also included in the 'Collection' principle in the model UPPs.[5] On 21 December 2001, the Privacy Commissioner made two Temporary Public Interest Determinations (TPIDs) in response to concerns that the long-standing and accepted practice of collecting health information about third parties—for example, family members—without their consent, for inclusion in the social and medical histories of health consumers may breach the NPPs.

63.4 The TPIDs were given effect for up to 12 months, to permit the Privacy Commissioner to conduct consultations on the issue. Over 60 submissions were received during the consultation period; and a conference was held in August 2002 to consider a draft determination.[6] The Privacy Commissioner formed the view that the collection of health information about third parties without consent in the course of delivering a health service was a breach of NPP 10.1, but that the act or practice should be allowed to continue. In the Privacy Commissioner's view, the public interest in its continuation substantially outweighed the public interest in adhering to NPP 10.1:

> The collection of family, social and medical history information is a critical part of providing assessment, diagnosis and treatment to individuals. The Commissioner acknowledged that obtaining the consent of third parties to collect their information, and notifying those individuals about these collections, would be impractical, inefficient and detrimental to the provision of quality health outcomes.[7]

63.5 In October 2002, the Privacy Commissioner made two public interest determinations (PIDs)—PID 9, in relation to the particular health service provider that made the original application; and PID 9A, in relation to health service providers generally—to replace the TPIDs. PIDs 9 and 9A were tabled in the Australian Parliament and took effect on 11 December 2002 for a period of up to five years.

---

3 Rec 63–5.

4 Rec 63–3.

5 The IPPs do not require that agencies have consent before collecting health information and so the same issue did not arise.

6 *Privacy Act 1988* (Cth) s 76 provides for a conference to be held to consider a draft determination on the Privacy Commissioner's initiative.

7 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 274.

Under PIDs 9 and 9A, health service providers could collect health information from health consumers about third parties without consent when both of the following circumstances were met:

- the collection of the third party's information into a health consumer's social, family or medical history was necessary to enable health service providers to provide a health service directly to the consumer; and

- the third party's information was relevant to the family, social or medical history of that consumer.[8]

63.6 The PIDs were reviewed in 2007; and PIDs 10 and 10A were issued with effect from 11 December 2007. PIDs 10 and 10A replaced PIDs 9 and 9A and were similar in scope, but expressly clarified that health service providers may collect third party information from a 'person responsible' for a health consumer where the health consumer is incapable of providing the information themselves. A 'person responsible' for an individual is defined in NPPs 2.5 and 2.6.

63.7 In the course of the OPC's review of the private sector provisions of the *Privacy Act 1988* (Cth) (the OPC Review)—which preceded the issue of PIDs 10 and 10A—the Privacy Commissioner considered whether the effect of PIDs 9 and 9A should be made permanent by an amendment to the *Privacy Act*. A number of submissions to the OPC Review commented on the effectiveness and importance of PIDs 9 and 9A and expressed support for such an amendment.[9] The OPC recommended that the Australian Government consider amending NPP 10 to include an exception that mirrors the operation of PIDs 9 and 9A.[10]

63.8 National Health Privacy Principle 1 (NHPP 1) of the draft *National Health Privacy Code* specifically provides for the collection of health information without consent where

> the information is a family medical history, social medical history or other relevant information about an individual, that is collected for the purpose of providing a person (including the individual) with a health service, and is collected by a health service provider:

---

8 Privacy Commissioner, *Public Interest Determination 9*, effective 11 December 2002; Privacy Commissioner, *Public Interest Determination 9A*, effective 11 December 2002.

9 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004; Mental Health Privacy Coalition, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

10 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 81.

(i) from the person who is to receive that service; or

(ii) from a relative or carer of the individual;[11] or

(iii) in any other situation, in accordance with any guidelines issued for the purposes of this paragraph.[12]

Issues Paper 31

63.9 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* should be amended to allow health service providers to collect information about third parties without their consent, in line with PIDs 9 and 9A. The ALRC also asked whether NHPP 1 of the draft *National Health Privacy Code* provided a more appropriate and effective framework for the collection of such information than the current provisions of the *Privacy Act*.[13]

63.10 A number of stakeholders, including the OPC, expressed support for amending the *Privacy Act* to give statutory effect to PIDs 9 and 9A.[14] The OPC noted that the PIDs were due to expire on 11 December 2007 and that no submissions to the OPC Review were critical of the content of the PIDs. The OPC suggested, however, that consideration might be given to limiting the provision to exclude genetic information and information in electronic health records, given the potential detail in such sources.[15]

63.11 The OPC also expressed a preference for the wording of the PIDs over the wording of NHPP 1 of the draft *National Health Privacy Code* on the basis that the health sector has been working with the wording of the PIDs for a number of years. The OPC suggested, however, that there may be merit in including the provision from the draft Code allowing collection of health information about third parties from 'a relative or carer of the individual'.[16] A number of other stakeholders expressed a preference for the wording in NHPP 1 of the draft Code.[17]

---

11 This paragraph would apply, for example, where the individual was a child or an adult with a decision-making disability. Handling the health information of children, young people and adults with a decision-making disability is discussed further in Part I of this Report.

12 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 1.1(i).

13 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–13.

14 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

15 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

16 Ibid.

17 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; A Smith, *Submission PR 79*, 2 January 2007.

63.12 The National Health and Medical Research Council (NHMRC) suggested that an amendment was needed to the notification requirements in NPP 1.5. NPP 1.5 requires that, where an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in NPP 1.3, such as the identity of the organisation and the purpose for which the information was collected. The NHMRC submitted that:

> NPP 1 should be amended to clarify that there may be circumstances in which it is reasonable for organisations to take no steps to ensure that an individual is:
>
> - notified of the fact that personal information about them has been collected from a third party; and/or
> - made aware of the specified matters relating to the collection and/or disclosure of that personal information.[18]

63.13 The NHMRC noted that the Privacy Commissioner had not included an exemption from the notification requirements in PIDs 9 and 9A. Instead, the Privacy Commissioner confirmed that, in the normal course of events, a health service provider will not be required to notify third parties that their health information has been collected for inclusion in the family, social or medical history of another individual.

> The NHMRC submits that it would be unreasonable to require notification in such circumstances. While notification in any individual case may be feasible, notification in relation to the vast number of patient encounters at which such information is collected would be administratively burdensome and practically impossible in many cases. In addition, a notification requirement would be likely, in many circumstances, to impair the provision by consumers to their health care providers of sensitive information about family members, which may be vital to their own health care.[19]

Discussion Paper proposal

63.14 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that PIDs 9 and 9A should be given statutory effect by being promulgated in the new *Privacy (Health Information) Regulations*.[20] This was on the basis that collection of health information about family members and others is routine practice and essential to provide appropriate health care to individuals.

63.15 The ALRC expressed the view that the proposed regulation should not exclude genetic information or information in electronic health records. Genetic information, because of its familial nature, is particularly important in family medical histories. The proposed regulation, however, was to be limited to collection of health information

---

18 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
19 Ibid.
20 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 57–3.

about third parties from the individual health consumer or a person who is 'responsible for' the individual, as discussed further below. This was intended to limit the amount and type of health information collected about third parties.

63.16 A regulation along these lines would not, for example, allow health service providers to collect health information from third party genetic samples. In addition, an individual health consumer generally will not have access to comprehensive genetic or electronic health records about third parties without their consent, and so will not be able to provide these to health service providers without the knowledge and consent of the third party.

63.17 The ALRC agreed that, in general, PIDs 9 and 9A were preferable to NHPP 1. The ALRC acknowledged, however, that the provisions in NHPP 1, allowing the collection of third party information from relatives and carers, were a valuable addition to the provisions in PIDs 9 and 9A.

63.18 The ALRC noted the concerns raised by the NHMRC in relation to the notification requirements in NPP 1.5. The ALRC agreed that it was unreasonable to require health service providers to notify third parties that personal information about them had been collected in the context of taking a family medical history. Under the 'Notification' principle—discussed in Chapter 23—where an agency or organisation collects personal information from an individual about a third party, the agency or organisation is required only to take such steps, if any, as are reasonable in the circumstances to notify the third party. Where personal information about third parties is collected by health service providers in these circumstances, it would be reasonable to take no steps to notify those third parties.

Submissions and consultations

63.19 There was general support for giving PIDs 9 and 9A statutory force.[21] The OPC agreed with the ALRC's reasoning in relation to genetic information, and expressed the view that such information should not be excluded from the provision. The OPC remained of the view, however, that collection from electronic health record systems should remain outside the provision.[22]

---

21 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Australian Medical Association, *Submission PR 524*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

22 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

63.20 The Australian Medical Association (AMA) agreed with the ALRC that third parties would not expect to be notified where personal information about them has been collected in the context of taking a family medical history.[23] The NHMRC stated that:

> We note that the ALRC agrees that it is unreasonable to require health service providers to notify third parties about whom health information has been collected in these circumstances. It would be helpful to include this advice in guidance supporting the *Privacy (Health Information) Regulations* to ensure clarity for providers.[24]

63.21 A number of stakeholders expressed support for allowing information about third parties to be collected from a person responsible for the health consumer.[25] The OPC noted that:

> PIDs 10 and 10A, issued by the Privacy Commissioner to replace PIDs 9 and 9A, permit the collection of third party health information for family, social or medical history purposes from an individual, *or* from a person 'responsible' for that individual where the individual is incapacitated. PIDs 9 and 9A did not expressly refer to collection from 'responsible' persons, although proposal 57–3 does so.[26]

63.22 On the other hand, Privacy NSW submitted that this proposed extension was too broad and that the provision should include a finite list of those from whom third party information can be collected.[27]

ALRC's view

63.23 The new *Privacy (Health Information) Regulations* should include provisions based on PIDs 10 and 10A. The content of these PIDs is premised on years of experience, consideration and review and has been found to be appropriate and effective. The new regulation should allow the collection of health information about third parties from the individual or a 'person responsible' for the individual. For example, it may be necessary to collect third party information from parents attending a health service with a child, or from a spouse or partner where the health consumer is unconscious. The concept of a 'responsible person' is discussed in detail below and includes family members, carers and legal guardians.[28] In the ALRC's view the recommended definition of a 'person responsible' is sufficiently clear and limited to be appropriate in these circumstances.

---

23 Australian Medical Association, *Submission PR 524*, 21 December 2007.
24 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
25 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.
26 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
27 Privacy NSW, *Submission PR 468*, 14 December 2007.
28 Rec 63–3.

Recommendation 63–1 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle, an agency or organisation that provides a health service may collect health information from an individual, or a person responsible for the individual, about third parties when:

(a) the collection of the third party's information is necessary to enable the health service provider to provide a health service directly to the individual; and

(b) the third party's information is relevant to the family, social or medical history of that individual.

Collection of family medical history information by insurance companies

63.24 A second issue raised in the OPC Review was the collection of third party health information without consent by insurance companies. In *Essentially Yours: the Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the NHMRC noted that:

> Insurance companies routinely collect family medical history information and use it in underwriting. The collection and use is based on the long recognised fact that certain diseases have a hereditary component, and that information about the medical history of family members is relevant in assessing the applicant's risk.[29]

63.25 The public interest issues to be considered in relation to the collection of this information by insurers are not the same as those considered in the development of PIDs 9 and 9A and PIDs 10 and 10A, which focused on collection by health service providers. The ALRC and AHEC suggested that it would be appropriate to consider the specific issues that arise in the insurance context in the course of a PID process, recommending that:

> Insurers should seek a Public Interest Determination under the *Privacy Act 1988* (Cth) in relation to the practice of collecting genetic information from applicants about their genetic relatives for use in underwriting insurance policies in relation to those applicants.[30]

---

29 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.49].

30 Ibid, Rec 28–3.

63.26 The OPC Review noted that the Privacy Commissioner had not yet considered an application for a PID in these terms[31] and recommended that:

> The Australian Government should consider undertaking consultation on limited exceptions or variations to the collection of family, social and medical history information, particularly with regard to genetic information and the collection practices of the insurance industry.[32]

63.27 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to allow insurance companies to collect health information about third parties without their consent in similar circumstances to those set out in PIDs 9 and 9A.[33] The ALRC did not include a specific proposal on this matter in DP 72.

Submissions and consultations

63.28 The Insurance Council of Australia expressed support for amending the *Privacy Act* to allow insurance companies to collect health information about third parties without their consent, noting that, 'in some instances health information of a third party is relevant to the medical history of a claimant and therefore required to properly manage and understand a claim'.[34] The Investment and Financial Services Association (IFSA) and a number of other stakeholders also expressed support for a specific exception.[35]

63.29 The Office of the Health Services Commissioner in Victoria noted that an amendment would be desirable to ensure that insurance companies only use third party information for the purpose of processing individual insurance contracts and claims, and in compliance with the *Privacy Act*. The Office submitted that 'clarity is needed in this area, and a working group should be set up to consult with stakeholders to come up with a suitable position on the issue'.[36]

63.30 By contrast, the OPC and other stakeholders did not support an exception to allow insurance companies to collect third party information without consent.[37] The OPC noted that the nature of the interests involved in the provision of health services

---

31 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 276.

32 Ibid, rec 82.

33 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–14.

34 Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

35 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

36 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

37 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Nursing Federation, *Submission PR 205*, 22 February 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; K Pospisek, *Submission PR 104*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007.

and the provision of insurance differ considerably. While PIDs 9 and 9A concern the collection of third party information for the preservation of life and health, the collection of such information by insurance companies involves actuarial decision making and risk management. The OPC expressed the view that, while important, 'the latter arguably lacks the compelling policy considerations necessary to warrant potentially lessening privacy protections'.[38]

63.31 The OPC noted that the IFSA *Family Medical History Policy* provides a practical solution to compliance with the *Privacy Act*. The Policy states that 'insurers will not collect family medical history information in an identifiable format'.[39] The OPC expressed support for this approach, which allows the insurance industry to collect relevant third party health information while complying with the requirements of the *Privacy Act*.

ALRC's view

63.32 The ALRC notes that the insurance industry has not yet applied to the Privacy Commissioner for a PID in relation to the collection of family medical history information without consent. IFSA's *Family Medical History Policy* appears to indicate that it is feasible for insurers to collect and use health information about third parties that does not identify them. If this is so, then amending the *Privacy Act* is unnecessary. If information collected by insurance companies is not 'about an individual whose identity is apparent, or can reasonably be ascertained, from the information', then it does not fall within the definition of 'personal information' and is not covered by the *Privacy Act.*

63.33 The ALRC notes, however, that the accompanying commentary in the IFSA *Family Medical History Policy* states that 'Family medical history information collected will be done on a de-identified basis, that is name and date of birth of the relative will not be collected.'[40] Collecting information without names and dates of birth attached may not be sufficient to ensure that information is not 'about an individual whose identity is apparent, or can reasonably be ascertained, from the information'. For example, if it is apparent from the information collected that the third party is the mother or father of the individual applying for insurance, the third party's identity can reasonably be ascertained from the information. In order to comply with the existing provisions of the *Privacy Act*, insurance companies must ensure that any third party health information they collect without consent is not about an individual whose identity is apparent or can reasonably be ascertained.

63.34 The ALRC is concerned that, although names and dates of birth are not collected, identities of third parties may be inferred from other information collected. If

---

38 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

39 Investment and Financial Services Association, *Family Medical History Policy: IFSA Standard No 16.00* (2005), [10.2].

40 Ibid, [10.2.1].

this is the case, insurance companies are collecting third party health information in breach of the *Privacy Act*. Insurers should seek a PID under the *Privacy Act* in relation to the practice. This is consistent with the relevant recommendation in ALRC 96,[41] discussed above.

Collection of health information as required or authorised by or under law

63.35 As noted above, NPP 10.1 provides, in part, that an organisation must not collect sensitive information, including health information, without consent except in a number of specified situations, including where 'the collection is required by law'.

63.36 NPP 10.2 provides a further exception to the general rule that health information must not be collected without consent. NPP 10.2 provides:

> Despite subclause 10.1, an organisation may collect health information about an individual if:
>
> (a) the information is necessary to provide a health service to the individual; and
>
> (b) the information is collected:
>
> (i) as required or authorised by or under law (other than this Act); or
>
> (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

63.37 NPP 10.2 recognises that health service providers may have legal obligations to collect certain health information without consent in the course of providing a health service. The OPC Guidelines note that 'law' includes Commonwealth, state and territory legislation, as well as the common law.[42] State and territory public health Acts, for example, require health service providers to collect and record certain information about health consumers with 'notifiable diseases', such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[43]

63.38 It is unclear why the language in NPP 10.1—'unless the collection is required by law'—and NPP 10.2—'where the information is collected as required or authorised by or under law'—is different. NHPP 1 of the draft *National Health Privacy Code* provides that health information may be collected without consent where the collection is 'required, authorised or permitted, whether expressly or impliedly, by or under law'.

---

41 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 28–3.

42 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 3. See also Ch 16.

43 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

Submissions and consultations

63.39 The OPC did not support the form of words in NHPP 1 on the basis that the formulation is too wide. The legal authority to collect health information without an individual's consent should be 'relatively narrow, transparent and subject to a clear statement from a Parliament'.[44]

63.40 The OPC expressed the view that the existing provisions in NPP 10.2—that allow health information to be collected without consent where necessary to provide a health service to the individual 'as required or authorised by or under law'—were appropriate. The OPC noted that the Prescription Shopping Information Service (PSIS)—established by Medicare Australia to allow registered medical practitioners to ring and find out if health consumers are 'prescription shopping' or acquiring medicines in excess of medical needs—is an example of collection that is authorised, rather than required, by or under law.[45]

63.41 The Department of Health and Ageing (DOHA) submitted that

> as a matter of general principle it should not be considered an interference with privacy for an agency or organisation to collect health information where 'the collection is required or authorised by law'.[46]

ALRC's view

63.42 The 'Collection' principle, discussed in detail in Chapter 21, provides that sensitive information, including health information, must not be collected without consent except where 'the collection is required or authorised by or under law'. The *Privacy Act* should not fetter a government's discretion to require or authorise that personal information, including health information, be handled in a particular way.[47] The 'required or authorised by or under law' exception in the 'Collection' principle is intended to replace the exceptions currently set out in NPP 10.1(b) and NPP 10.2. This will eliminate the problem of inconsistency between these two existing provisions.

Binding rules established by health or medical bodies

63.43 NPP 10.2 also provides that health information may be collected without consent if the information is collected in order to provide a health service to the individual and in accordance with binding rules established by 'competent health or medical bodies that deal with obligations of professional confidentiality'. The draft *National Health Privacy Code* does not include this exception.

---

44 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
45 *National Health Act 1953* (Cth) s 135AC.
46 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.
47 See Ch 16 for a detailed discussion of this issue.

63.44 The OPC Review recommended that:

> The Australian Government should consider amending NPP 10.2(b)(ii) to clarify the nature of the binding rules intended to be covered by this provision, particularly with regard to the substantive content of such rules.[48]

63.45 The OPC's submission considered the exception provided by NPP 10.2(b)(ii), arguing that such rules would need to:

- be formally adopted by a state or territory medical board as a statement of appropriate professional practice;
- prescribe the circumstances in which the collection can occur without the patient's consent;
- define or regulate obligations of professional confidentiality in relation to the information collected; and
- provide a mechanism for sanctions for breach.

63.46 The OPC stated that:

> NPP 10.2(b)(ii) is intended to provide a mechanism to allow collection by health service providers where necessary to provide a health service, and in accordance with binding rules of professional confidentiality. However, it is the Office's view that no current rules fit the terms of 10.2(b)(ii) in such a way that it could be confidently relied upon.[49]

63.47 The NHMRC submitted that no such rules existed, and that the provision should be deleted.[50]

ALRC's view

63.48 Both the OPC and the NHMRC stated that they were not aware of any existing 'rules established by competent health or medical bodies that deal with obligations of professional confidentiality' that would fulfil the requirements of NPP 10.2(b)(ii). No such rules were drawn to the attention of the ALRC in the course of this Inquiry, and no objections were raised in response to the ALRC's view, expressed in DP 72, to leave these provisions out of the 'Collection' principle. Consequently, the ALRC has not included this mechanism in the 'Collection' principle.

---

48 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 84.

49 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

50 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

Difference between the collection, use and disclosure principles

63.49 Another issue raised in IP 31 was a discrepancy in approach between NPP 2 on the use and disclosure of sensitive information, and NPP 10 on collection of sensitive information.[51] In many communications of health information, there is both a disclosure and a collection. For example, a general practitioner collects health information for the primary purpose of providing a health service to a health consumer. The general practitioner may disclose that information to a number of other health service providers involved in treating the consumer, for example, a pathologist and a specialist.

63.50 Such disclosures are consistent with NPP 2 if they are directly related to the primary purpose of collection and within the reasonable expectations of the individual health consumer. NPP 10 requires that health information be collected with consent, although that consent may be express or implied. The issue is whether the pathologist and the specialist in the above example can rely on the implied consent of the health consumer to collect the consumer's health information.

63.51 To better align the use and disclosure of health information under NPP 2 and collection of health information under NPP 10, the OPC suggested that NPP 10 should be amended to allow the collection of health information where necessary for providing a health service and where the collection was within the expectations of a reasonable person:

> In the Office's view, option 3 would appear to offer an appropriate and transparent mechanism for reforming NPP 10.2(b)(ii), and would cause the least interference with current good practice in the health sector. This option would provide greater alignment between the disclosure and collection provisions of the NPPs, and resolves the possible uncertainty surrounding collection by members of a treating team and other similar scenarios.[52]

63.52 A number of other stakeholders also suggested that this matter should be clarified.[53]

Discussion Paper proposal

63.53 In DP 72, the ALRC noted that health information must be collected with consent—except in specified circumstances—and that consent, to be valid, must be voluntary and informed.[54] If health information is used or disclosed for the primary purpose of collection or for a directly related secondary purpose and the individual would reasonably expect the health service provider to use or disclose the information in that way, the ALRC expressed the view that the resulting collection by another

---

51 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [8.160].

52 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

53 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

54 See Ch 19 for a detailed discussion of consent.

member of the treating team, for example, a pathologist or specialist, is likely to be consistent with the express or implied consent provided at the point of original collection. Good communication between health service providers and consumers at the point of original collection would put this beyond doubt.

63.54 The ALRC recognised, however, that it is important to facilitate information flow in the health services context among members of treatment teams. The ALRC asked whether the proposed *Privacy (Health Information) Regulations* should provide that health information may be collected without consent where it is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information.[55] A regulation of this nature would bring the 'Collection' principle, as it applies to health information, more into line with the 'Use and Disclosure' principle.

Submissions and consultations

63.55 A significant number of stakeholders expressed support for bringing the 'Collection' principle and the 'Use and Disclosure' principle into line in this way.[56] The NHMRC stated that this was clearly in the interests of health consumers.[57] Avant Mutual Group Ltd agreed, noting that:

> Medical care is often delivered by a number of healthcare professionals. An individual will reasonably expect that a medical specialist will write to his GP following a consultation. Another example is a patient being discharged from hospital. A discharge summary will be sent to the plaintiff's treating GP and/or specialists. The individual would reasonably expect his/her GP and other treatment providers to be kept appraised of the treatment he/she received at the hands of the specialist or whilst in hospital in order to ensure continuity of care. Avant has noted with some dismay that some health organisations have already adopted practices that impede the proper flow of information between healthcare professionals treating the same patient because of the organisation's misapprehension of contemporary privacy laws. An example is the increasing practice of hospitals to require written consent from patients before important but routine health information is disclosed to the patient's nominated general practitioner.[58]

---

55 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 57–1.

56 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

57 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

58 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

63.56 On the other hand, a number of stakeholders expressed concern about this issue. Medicare Australia stated that:

> This question refers to collection without consent in order to provide a health service where the person would reasonably expect the information to be collected for that purpose. It might be more appropriate to suggest that such information would be collected with implied consent, and that the person should be asked for specific consent if there is doubt about whether consent would be provided.
>
> It is important to note that health information should not be collected without either express or implied consent.[59]

63.57 One stakeholder thought that the proposed formulation was too wide. It suggested that a more appropriate approach would be to allow the collection of health information without consent where:

- it is necessary to provide a health service to the individual; and
- the collection results from the disclosure by another health service provider for a directly related secondary purpose within the reasonable expectations of the individual; or
- where it is impracticable to obtain the individual's consent; or
- the individual is incapable of providing consent and it is not possible to obtain consent from a responsible person or authorised representative on behalf of the individual.[60]

63.58 Privacy NSW submitted that it would be difficult for health service providers to know whether the collection was within the reasonable expectations of the individual.[61]

ALRC's view

63.59 As noted above, it is possible to argue that the sharing of an individual's health information among a team of health service providers treating the individual is done on the basis of express or implied consent—in which case, the privacy principles do not require amendment. It is important to be clear in the health services context, however, that the collection, use and disclosure of such information by members of the treating team are supported by the 'Collection' principle and the 'Use and Disclosure' principle where the collection, use or disclosure would fall within the reasonable expectations of the individual.

63.60 The new *Privacy (Health Information) Regulations* should provide that an agency or organisation that is a health service provider may collect health information about an individual, if the information is necessary to provide a health service to the individual and the individual reasonably would expect the agency or organisation to

---

59 Medicare Australia, *Submission PR 534,* 21 December 2007.
60 Confidential, *Submission PR 570,* 13 February 2008.
61 Privacy NSW, *Submission PR 468,* 14 December 2007.

collect the information for that purpose. The recommended provision is not too wide, as it is limited to the collection of health information in the health services context and is linked to the reasonable expectations of the individual. The provision is intended to ensure that health service providers are confident to collect information where necessary to provide a health service to the individual, in circumstances in which the individual would expect them to do so.

63.61 Health service providers will be required to exercise judgement in relation to the reasonable expectations of the individual. The ALRC notes that the OPC has issued guidance in relation to the use and disclosure of health information in the health services context for a directly related secondary purpose that is within the reasonable expectations of the individual.

> A patient's expectations can be effectively managed through good provider–patient communication. This usually means the patient has been told the use or disclosure would happen, or they would expect it to happen because of why they gave the information to the provider in the first place.[62]

63.62 The guidance goes on to suggest that the usual starting point for assessing a health consumer's reasonable expectations is what an ordinary individual would expect to happen to their health information in the given circumstances. A great deal of this guidance would be relevant to the collection of health information in the health services context. The ALRC anticipates that the OPC would revisit the guidance following the implementation of the recommendations in this Report.

Recommendation 63–2 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle, an agency or organisation that is a health service provider may collect health information about an individual if the information is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose.

Use and disclosure of health information

Use and disclosure for primary and secondary purposes

63.63 IPPs 10 and 11 and NPP 2 regulate the use and disclosure of personal information. IPP 10 provides that information, including health information, may be used for the purpose it was collected or a directly related purpose. If it is to be used for

62 Office of the Privacy Commissioner, *Sharing Health Information to Provide a Health Service*, Information Sheet 25 (2008).

any other purpose the person who wishes to use the information must have the consent of the individual concerned. IPP 11 provides that information may not be disclosed to a person, body or agency unless the individual concerned is reasonably likely to have been aware that information of that kind is usually passed to that person, body or agency. Otherwise, the person who wishes to disclose the information must have the consent of the individual concerned. There are several exceptions to these rules, including where use or disclosure of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

63.64 NPP 2 provides that sensitive information, including health information, may be used or disclosed for the 'primary purpose of collection' or a secondary purpose where the secondary purpose is directly related to the primary purpose of collection and the individual concerned would reasonably expect the organisation to use or disclose the information for that secondary purpose. If it is to be used for any other purpose the person who wishes to use the information must have the consent of the individual concerned. There are several exceptions to this rule, including where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety.

63.65 Concern was expressed in the course of the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry)[63] and the OPC Review[64] that the concept of 'primary purpose of collection' in NPP 2 may be interpreted in a narrow way and impede the provision of holistic health care and the appropriate management of an individual's health.

63.66 In its submission to the OPC Review, the AMA expressed the view that the primary purpose of collection should be 'to provide for the person's health care and general well being … unless another meaning is specifically agreed to between the doctor and the patient'. The AMA also noted that the primary purpose should not be limited to a particular episode of care:

> The care of a patient's health and well being is not achieved by episodic care. The process is not static, nor can it be temporally defined. One's past health and well being impacts on one's current health and well being which in turn influences one's future health and well being.[65]

---

63 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.63].

64 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 264–265.

65 Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

63.67 The OPC Review noted that:

> There is an intentionally close relationship between the primary purpose and the directly related purpose provisions at NPP 2.1(a), which in this context means that with open communication between a health service provider and an individual (something to be expected in the delivery of quality health care), a holistic approach to care can be agreed either explicitly or implicitly. In other words, where the individual expects their health information to be used in the delivery of health care to them in a holistic manner, it is permissible under NPP 2.[66]

63.68 The OPC Review stated that the OPC would work with the health sector to develop further guidance about the operation of NPP 2 as it specifically relates to the issue of primary and secondary purpose in the health services context.[67]

63.69 The regime established for using and disclosing health information in NHPP 2 of the draft *National Health Privacy Code* is similar to NPP 2, in that it allows the use and disclosure of health information for the primary purpose of collection and directly related secondary purposes within the reasonable expectations of the health consumer. However, NHPP 2 also allows the use of health information without consent where all of the following apply:

> (i) the organisation is a health service provider providing a health service to the individual; and
>
> (ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and
>
> (iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and
>
> (iv) the information is used in accordance with guidelines, if any, issued for the purposes of this paragraph.

63.70 In IP 31, the ALRC asked whether guidance by the OPC was an appropriate and effective response to concerns about the provisions of NPP 2 and the use and disclosure of health information.[68]

Submissions and consultations

63.71 The NHMRC's submission described a number of situations in which health service providers might be unclear about their obligations under the *Privacy Act*:

> For example, a patient is admitted to a hospital for acute care, and the hospital contacts the patient's general practitioner and asks him or her to disclose health information about the patient for the purpose of ongoing clinical care. There is not a

---

66 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 263.

67 Ibid, recs 77–78.

68 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–17.

> serious and imminent threat to the patient's life, health or safety. The general practitioner does not have direct access to the patient to obtain consent to the disclosure of their health information. Nevertheless, good clinical practice requires its timely disclosure.[69]

63.72 The NHMRC stated that, while use or disclosure in these circumstances might well be a directly related secondary purpose, it will not always be clear to general practitioners whether individuals would reasonably expect their health information to be disclosed in these circumstances. The NHMRC was of the view, therefore, that use and disclosure to other health care providers of health information for the purposes of the current care of an individual health consumer should be permitted explicitly without any additional requirement that the health consumer would reasonably expect the information to be used or disclosed in this way.[70]

63.73 The Australian Nursing Federation (ANF) submitted, however, that if health information is collected with consent and appropriate information is provided to individuals, 'then there should be little impediment to the appropriate management of the individual's health'.[71]

63.74 The OPC remained of the view that NPP 2 sits comfortably with the 'relationships of trust and good communication that are the hallmark of good practice in the health sector' and that NPP 2 does not require amendment. The OPC suggested that it is not always, or even usually, necessary for health service providers to seek the consent of an individual before using or disclosing their health information to other members of a treatment team.[72]

63.75 The OPC also argued that a holistic approach to the provision of health services can be accommodated by the 'directly related secondary purpose within the reasonable expectations of the individual' test in NPP 2. The OPC noted that this test is consistent with the ethical principles set out in the AMA's Code of Ethics,[73] including respect for the individual; health care as a collaboration between doctor and patient; and patient confidentiality. The OPC did not agree that the primary purpose of collection should be broadly defined as providing 'for the person's health care and general well being', as this would allow use and disclosure of health information without taking the health consumer's reasonable expectations into account or, alternatively, seeking consent.

63.76 The OPC was not of the view that NHPP 2 provided a better framework for the use and disclosure of health information. The OPC stated that NHPP 2 was unnecessarily lengthy and complex, and that the discretions conferred by the provision

---

69 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
70 Ibid.
71 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.
72 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
73 Australian Medical Association, *Code of Ethics* (2004).

did not give adequate weight to individuals' wishes and expectations about the way that their health information is used and disclosed.

63.77 A number of other stakeholders, however, were more supportive of NHPP 2.[74] One stakeholder expressed support on that the basis that NHPP 2 provides clearer guidance on when it is appropriate to use and disclose health information in the health services context, particularly in relation to ongoing health care.[75]

63.78 The OPC reiterated the recommendations from its review that further guidance on the operation of NPP 2 in the health services context would be provided:

> This may include updating information sheets, providing greater access to these and other Office resources, and publishing articles in prominent health sector publications. A clearer understanding of how these terms operate would allow health service providers to be more confident in using and disclosing patients' information for appropriate and mutually anticipated purposes, and ensure individuals receive enough information to retain control over the direction of their healthcare.[76]

63.79 A number of other stakeholders agreed that further guidance was necessary and appropriate.[77]

Discussion Paper 72

63.80 The ALRC did not make a proposal in relation to this issue in DP 72, but expressed support for the OPC Review recommendation that further guidance be developed for health care providers on the use and disclosure of health information in the provision of health services. The ALRC perceived a lack of clarity on the meaning of the principles among health service providers, which is particularly undesirable if it is preventing the flow of health information from one health service provider to another in appropriate circumstances.

ALRC's view

63.81 The ALRC notes that the OPC recently issued detailed guidance on the use and disclosure of health information in the health services context. Information Sheet 25, *Sharing Health Information to Provide a Health Service*, includes guidance on the meaning of 'directly related purpose' and notes that, in the health services context, directly related purposes 'are likely to include anything to do with the patient's care or

---

74 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

75 Confidential, *Submission PR 570,* 13 February 2008.

76 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

77 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; A Smith, *Submission PR 79,* 2 January 2007.

wellbeing'.[78] The Information Sheet also discusses how to establish an individual's reasonable expectations and includes a series of case studies to illustrate how the principle might operate in practice.

63.82 The test set out in NPP 2 and incorporated in the 'Use and Disclosure' principle—that the use or disclosure of health information must be for the primary purpose of collection or a directly related secondary purpose within the reasonable expectations of the individual—is appropriate and workable in the health services context. An individual's health information should not be used or disclosed in ways that are outside his or her reasonable expectations, except in very specific circumstances. These circumstances are set out in the exceptions to the 'Use and Disclosure' principle, for example, where the use or disclosure is required or authorised by or under law.

63.83 The regulation recommended above—to allow health service providers to collect health information if the information is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose—in combination with detailed guidance from the OPC on the sharing of information in the health services context, will address the issues identified by stakeholders in the course of this Inquiry.

Disclosure to a person responsible for an individual

63.84 NPP 2.4 makes special provision for the disclosure of health information to 'a person who is responsible for the individual', where the individual is physically or legally incapable of giving consent to the disclosure or physically cannot communicate this consent. Such disclosures may only be made by health service providers in the health services context. The health service provider must be satisfied that the disclosure is necessary to provide appropriate care or treatment to the individual or the disclosure must be made for compassionate reasons. The disclosure must not be contrary to any wish expressed by the individual—before the individual became unable to give or communicate consent—of which the health service provider is aware or could reasonably be expected to be aware. The disclosure must be limited to that information that it is reasonable to disclose in the circumstances.

63.85 NPPs 2.5 and 2.6 define 'a person who is responsible for the individual' as:

- a parent of the individual;
- a child or sibling of the individual and at least 18 years old;
- a spouse or de facto spouse of the individual;

---

78 Office of the Privacy Commissioner, *Sharing Health Information to Provide a Health Service*, Information Sheet 25 (2008).

- a relative of the individual, at least 18 years old and a member of the individual's household;
- a guardian of the individual;
- exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;
- a person who has an intimate personal relationship with the individual; or
- a person nominated by the individual to be contacted in case of emergency.[79]

Discussion Paper proposals

63.86 In DP 72, the ALRC proposed a number of changes to the NPPs dealing with 'a person responsible for the individual'. The first proposal was that the provisions should be moved to the new *Privacy (Health Information) Regulations* and should be expressed to apply to agencies and organisations. The relevant NPPs only deal with health information in the health services context and, as discussed in Chapter 60, the ALRC's view is that such provisions should not be included in the body of the UPPs but should be set out in regulations expressed to amend the UPPs.

63.87 In DP 72, the ALRC also proposed that the *Privacy Act* be amended to include an 'authorised representative' mechanism. Where an individual was incapable of giving consent, making a request or exercising a right under the Act, the ALRC proposed that an 'authorised representative' of that individual be allowed to make these decisions on behalf of the individual. An 'authorised representative' was to be defined as a guardian appointed under law; a guardian appointed under an enduring power of attorney; a person with parental responsibility for the individual; or otherwise empowered under law to act as agent in the best interests of the individual.[80] As a consequence, the ALRC also proposed that the definition of 'a person responsible for the individual' be amended to include a reference to an 'authorised representative'.[81]

63.88 In order to provide consistency across federal legislation, the ALRC also proposed that the reference to 'de facto spouse' in NPP 2.5 should be changed to 'de facto partner', in line with recommendations made in the report, *Uniform Evidence Law* (ALRC 102).[82]

---

79 The terms 'child', 'parent', 'relative' and 'sibling' are defined in NPP 2.6.

80 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 61–2.

81 Ibid, Proposal 57–4(c).

82 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Rec 4–4.

Submissions and consultations

63.89 A number of stakeholders expressed support for these proposals.[83] Carers Australia noted that the provisions allow information to flow to family members and carers in appropriate circumstances:

> Historically, the privacy legislation has had unintended consequences especially in restricting carers' access to information which is necessary to perform their caring role. There is a mounting body of evidence that suggests carer participation in assessment, treatment and care planning is critical in both the treatment and recovery of the person and the wellbeing of the carer. This has particularly been demonstrated in the area of mental health. In the same way that the potential for negative outcomes for an individual occur as a result of a restriction of the sharing of information between treating teams, the same risks exist if information is not adequately shared with carers as they are the major providers of support to people with disability, illness or injury.[84]

63.90 Carers Australia noted that NPP 2.4(b) currently refers to a person providing a health service as a 'carer' and suggested that a more appropriate term would be 'health service worker' or something similar. The OPC agreed with this view, stating that:

> The Office is aware that some terminology used in NPP 2.4 may be a source of confusion to providers and others. In particular, NPP 2.4 uses the term 'carer' to signify the health professional who is providing care, rather than the everyday usage of that term, which generally aligns more with the person 'responsible' for the individual.[85]

63.91 Carers Australia also expressed concern about NPP 2.4(c), which provides that disclosures can be made if they are not contrary to the expressed wishes of the individual. Carers Australia noted that this provision may give rise to difficulties, especially in the mental health area, where individuals may experience paranoia about the motives of family, friends and carers, or may be in denial about their condition:

> Despite having had a positive relationship with their family in the past, they may request that information is not provided to them. While this is the person's expressed wish, it is doubtful if they currently have the capacity to make that decision. Whilst the legislation would still allow for the provision of information to families and friends, the interpretation of health service workers routinely denies families information in such situations.[86]

63.92 The NHMRC stated that it was important to ensure that information can be disclosed to an individual's primary carer, even where that carer is not a relative and

---

83 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

84 Carers Australia, *Submission PR 423*, 7 December 2007.

85 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

86 Carers Australia, *Submission PR 423*, 7 December 2007.

does not hold a legal power of attorney or guardianship order. The NHMRC pointed to the *Guardianship and Administration Act 1986* (Vic), which defines 'primary carer' as 'any person who is primarily responsible for providing support or care to a person'.[87]

63.93 The ACT Government Department of Disability, Housing and Community Services drew attention to the provisions of the *Health Records (Privacy and Access) Act 1997* (ACT). This Act allows disclosures to 'a person responsible for the consumer's care' where 'in the record keeper's opinion, the disclosure is necessary to enable the carer to safely and effectively provide appropriate services to, or care for, the consumer'. The Department added that:

> In regard to multiple carers and the *Review of Australian Privacy Laws*, the Department recommends ensuring multiple carers are recognised, in particular young carers, in the flow of information between health service providers. Increasingly young people are taking on the primary caring responsibilities for their parents and siblings.[88]

63.94 The OPC also drew attention to carers under the age of 18, stating that:

> In particular, the Office notes that while NPP 2.5 refers to children 'at least 18 years of age', a significant number of carers are under 18 years of age, including some primary carers. Carers Australia provides anecdotal evidence that young carers may in some cases be 'overlooked or not consulted by health practitioners in discussions about the care or treatment of the person they care for, because they are children'. Unless carers under 18 years are recognised as 'authorised representatives', they would not be able to receive information from providers for treatment or compassionate reasons under NPP 2.4 or its equivalent.[89]

ALRC's view

63.95 It is important to include provisions in the new *Privacy (Health Information) Regulations* allowing disclosures of health information in the health services context to people who are responsible for an individual where the individual is incapable of providing consent to the disclosure. The regulations should be modelled on the existing NPPs 2.4 to 2.6 with the following amendments.

63.96 The regulations should be expressed to apply to agencies and organisations as both provide health services and regularly interact with health consumers, their families, legal representatives and carers. The regulations should allow disclosures to any person who is 'primarily responsible for providing support or care to the individual'. The current provisions do not cover a sufficiently wide range of carers; for example, they may not cover family friends performing caring responsibilities or paid

---

87 *Guardianship and Administration Act 1986* (Vic) s 3.

88 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.

89 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

professional carers. For the reasons put forward by Carers Australia and the OPC, above, the provisions should not use the term 'carer' to refer to the health service provider.

63.97 The ALRC notes the difficulties raised by Carers Australia in relation to the requirement that the disclosure must not be contrary to the expressed wishes of the individual. This is, however, an appropriate limit on the provisions. If an individual has requested that personal health information not be disclosed to a particular person, that request should be respected. It is a matter for health service providers' judgement as to whether an individual had capacity to make that decision at the time it was expressed.

63.98 For the reasons discussed in Chapter 70, the ALRC no longer supports the introduction of the 'authorised representative' mechanism into the *Privacy Act.* Instead, the new regulations should refer to 'a substitute decision maker authorised by a federal, state or territory law to make decisions about the individual's health'.

63.99 The ALRC also recommends that there should be no express age limit included in the definition of 'a person responsible for an individual'. Children and other family and household members under 18 often play the role of primary carer. Health service providers should have the discretion to disclose an individual's health information to these people in the circumstances set out in NPP 2.4. In considering whether to disclose an individual's health information to a person who is under the age of 18, a health service provider should consider, on a case-by-case basis, that person's maturity and capacity to understand the information.

63.100 Finally, the *Privacy Act* should be amended to refer to 'de facto partner' rather than 'de facto spouse'. The Act should define 'de facto partner' as 'a person in a relationship as a couple with another person to whom he or she is not married'. This is consistent with the ALRC's recommendations in ALRC 102.[90]

Recommendation 63–3 National Privacy Principles (NPPs) 2.4 to 2.6—dealing with the disclosure of health information by a health service provider to a person who is responsible for an individual—should be moved to the new *Privacy (Health Information) Regulations*. The new regulations should provide that, in addition to the other provisions of the 'Use and Disclosure' principle, an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual, if the individual is incapable of giving consent to the disclosure and all the other circumstances currently set out in NPP 2.4 are met. In addition, the new regulations should:

90 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Recs 4–4, 4–5.

(a) be expressed to apply to both agencies and organisations;

(b) not refer to a health service provider who may make a disclosure under these provisions as a 'carer'; and

(c) define 'a person who is responsible for an individual' as:

(i) a parent, child or sibling of the individual;

(ii) a spouse or de facto partner of the individual;

(iii) a relative of the individual who is a member of the individual's household;

(iv) a substitute decision maker authorised by a federal, state or territory law to make decisions about the individual's health;

(v) a person who has an intimate personal relationship with the individual;

(vi) a person nominated by the individual to be contacted in case of emergency; or

(vii) a person who is primarily responsible for providing support or care to the individual.

In considering whether to disclose an individual's health information to a person who is responsible for an individual and who is under the age of 18, a health service provider should consider, on a case-by-case basis, that person's maturity and capacity to understand the information.

Recommendation 63–4 The *Privacy Act* should be amended to provide a definition of 'de facto partner' in the following terms: 'de facto partner' means a person in a relationship as a couple with another person to whom he or she is not married.

Use and disclosure of genetic information

63.101 The *Privacy Legislation Amendment Act 2006* (Cth), passed in September 2006, amended NPP 2.1 to allow the use or disclosure of an individual's genetic information, without consent, where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative of the individual. Any such use or

disclosure must be done in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner.[91] In February 2008, the NHMRC issued draft guidelines for public consideration and comment.[92]

Discussion Paper proposal

63.102 In DP 72, the ALRC proposed that this provision be moved to the new *Privacy (Health Information) Regulations* and that the regulation should be expressed to apply to both agencies and organisations. In DP 72, the ALRC also proposed that, where guidelines are intended to be binding, they should be called 'rules',[93] and that the rules to be issued in relation to the use and disclosure of genetic information should be issued by the Privacy Commissioner.[94]

63.103 A number of stakeholders expressed support for these proposals.[95] The NHMRC noted that the relevant rules should be developed in close consultation with the NHMRC.[96] The OPC was of the view that the rules should be issued by the NHMRC and approved by the Privacy Commissioner.[97]

ALRC's view

63.104 'Health information' is defined to include genetic information in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. Currently, provisions relating to the use and disclosure of genetic information where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative are included in the NPPs. As the provisions relate to the use and disclosure of a form of health information obtained in the health services context, the ALRC recommends that they should be included in the new *Privacy (Health Information) Regulations.*

63.105 The use and disclosure of genetic information in these circumstances would normally be in breach of the UPPs. In this respect, the new regulation will be similar in effect to PIDs. As discussed in detail in Chapter 47, PIDs are developed and 'made' by the Privacy Commissioner. This level of involvement and control by the regulator is appropriate in circumstances where the level of protection provided by the UPPs is to be modified. By way of contrast, privacy codes, developed by industry and 'approved'

---

91 *Privacy Act 1988* (Cth) s 95AA. This amendment was intended to implement, in part, Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 21–1.

92 National Health and Medical Research Council, *Disclosure of Genetic Information to a Patient's Genetic Relatives Under Section 95AA of the Privacy Act 1988 (Cth): Guidelines for Health Practitioners in the Private Sector*, Consultation Draft (2008).

93 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–2.

94 Ibid, Proposal 57–5.

95 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

96 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

97 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

by the Privacy Commissioner, cannot derogate from the protection provided by the UPPs. This distinction is appropriate. Where collection, use and disclosure of personal information are to be allowed in circumstances that derogate from the UPPs, the Privacy Commissioner should retain primary responsibility for the development and issue of the rules that regulate that activity.

63.106 The guidelines, currently issued under s 95AA of the *Privacy Act*, are intended to be binding and to form part of the legal framework within which genetic information may be used and disclosed. The ALRC considers that the 'rules' which would replace the 'guidelines' should be formally issued by the Privacy Commissioner. The Privacy Commissioner would be free to develop the rules in consultation with the NHMRC and other relevant stakeholders.

Recommendation 63–5 The new *Privacy (Health Information) Regulations* should include provisions similar to those set out in National Privacy Principle 2.1(ea) on the use and disclosure of genetic information where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. These regulations should apply to both agencies and organisations. Any use or disclosure under the new regulations should be in accordance with rules issued by the Privacy Commissioner.

Access to health information

Background

63.107 In *Breen v Williams*,[98] the High Court of Australia unanimously held that health consumers do not have a right of access to their medical records as a matter of common law. Consequently, health consumers must rely on legislation, including the *Privacy Act*, to provide them with a right of access to the health information held in medical records.

63.108 IPP 6 provides in relation to agencies that:

> Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

63.109 The exceptions to IPP 6 include, for example, those situations in which a record-keeper is required or authorised to refuse access under the *Freedom of*

98 *Breen v Williams* (1996) 186 CLR 71.

Information Act 1982 (Cth) (the FOI Act) and the *Archives Act 1983* (Cth). Chapter 15 considers how this legislation, including the exemptions set out in the legislation, interacts with the *Privacy Act*.

63.110 NPP 6 provides that organisations must provide individuals with access to their personal information on request, subject to a number of exceptions. In the case of health information, organisations are not required to provide access if doing so would pose a serious threat to the life or health of any individual.[99] The list of exceptions also includes situations in which: providing access would have an unreasonable impact on the privacy of other individuals;[100] the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery;[101] and denying access is required or authorised by or under law.[102]

63.111 The draft *National Health Privacy Code* provides very detailed provisions on providing access to health information and for dealing with situations in which access is refused. As discussed in Chapter 60, this level of detail should not be included in a principles-based regime, but could be included in guidelines as suggested best practice. The grounds provided in NHPP 6 for refusing access are essentially the same as those provided in NPP 6.[103]

63.112 Both health consumers and health service providers appear to have concerns relating to access to health information. Of the 330 complaints under the NPPs against health care providers received by the OPC between 21 December 2001 and 31 January 2005, roughly half (163) concerned a refusal of access to health records.[104]

Breakdown in therapeutic relationship

63.113 In the course of the OPC Review, the AMA and the Mental Health Privacy Coalition expressed concern that, in the health care context, there are occasions when providing access to medical records could cause harm to the health consumer or interfere with the therapeutic relationship between a health consumer and a health service provider.[105] The OPC Review stated that access issues can cause breakdowns in therapeutic relationships and that this may give rise to a serious risk to patient health.[106]

---

99 *Privacy Act 1988* (Cth) sch 3, NPP 6.1(b).
100 Ibid sch 3, NPP 6.1(c).
101 Ibid sch 3, NPP 6.1(e).
102 Ibid sch 3, NPP 6.1(h).
103 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 6.1.
104 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 112.
105 Ibid, 115.
106 Ibid, 117.

63.114 The OPC expressed the view that NPP 6.1(c)—which allows an organisation to deny access where it would have an unreasonable impact on the privacy of someone else—might be relied upon to protect health service providers' views in some circumstances. The OPC did not address the situation in which providing access might cause a breakdown in the therapeutic relationship, but would not pose a serious threat to the life or health of an individual. The OPC did not recommend an amendment to NPP 6,[107] but has issued further guidance in an information sheet on this matter: *Denial of Access to Health Information due to a Serious Threat to Life or Health*.[108]

Issues Paper 31

63.115 In IP 31, the ALRC asked whether the exception in NPP 6.1(b)—that allows access to be denied if it would pose a serious threat to the life or health of any person—was appropriate. The ALRC asked whether the exception should be extended to allow a health service provider to deny access to health information if providing access would pose a threat to the therapeutic relationship between the health service provider and the health consumer.[109]

Submissions and consultations

63.116 There was strong support among stakeholders for the existing exception in NPP 6.1(b)[110] and little support for extending the exception to include threats to the therapeutic relationship alone. A number of submissions noted that, while denying access to health information can damage therapeutic relationships, health consumers are at liberty to change health service providers if the relationship does break down. The ANF was strongly of the view that:

> This exception should **NOT** be extended to allow a health service provider to deny access to health information if providing access to the information would pose a threat to the therapeutic relationship between the health service provider and the health consumer. If the therapeutic relationship is so fragile then it is not going to be improved if the health service provider refuses to provide access. There is also the potential for a person to deny access for an improper purpose eg the information reveals an adverse event, inappropriate care or treatment or other information that a person may be entitled to have.[111]

---

107 Ibid, rec 30.

108 Office of the Privacy Commissioner, *Denial of Access to Health Information Due to a Serious Threat to Life or Health*, Private Sector Information Sheet 21 (2008).

109 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–20.

110 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

111 Australian Nursing Federation, *Submission PR 205*, 22 February 2007.

63.117 The OPC stated that NPP 6.1(b) is an appropriate and effective exception, and should not be extended to include threats to the therapeutic relationship alone.

> The fact that the threat must be 'serious' reflects the principle that access to one's own personal information should be the rule, rather than the exception. At the same time the exception is broad enough to encompass serious threats to any relevant person (including threats to mental health), such as the individual themselves, other patients, practitioners and staff, and the individual's family. Similar language is used in the equivalent exceptions under NSW and Victorian health records legislation.[112]

63.118 The OPC suggested, however, that the phrase 'would pose a serious threat' in NPP 6.1(b), requires a degree of certainty that may not always be achievable in clinical environments. It is not always possible to predict how a health consumer will react to being granted access to their health information. On this basis, the OPC suggested an alternative test of 'reasonably likely to pose a serious threat to the life or health of any individual'.

ALRC's view

63.119 There was little support for extending the exception in NPP 6.1(b) to include a threat to the therapeutic relationship, and the ALRC view is that there is no case to recommend this change.

63.120 The ALRC agrees with the OPC that the current test—'providing access would pose a serious threat to the life or health of any individual'—requires a level of certainty that may be very difficult to establish. The 'Access and Correction' principle, discussed in detail in Chapter 29, has adopted the approach suggested by the OPC. The principle provides in part that, if an individual requests access to personal information, an agency or organisation must respond within a reasonable time and provide the individual with access to the information except to the extent that:

- in the case of an agency, the agency is required or authorised to refuse to provide the individual with access under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents. Under this exception, agencies may deny an individual access on the basis of exceptions set out in the FOI Act. The FOI Act provides that access may be denied where disclosure 'would, or could reasonably be expected to endanger the life or physical safety of any person';[113] and

- in the case of an organisation, providing access would be reasonably likely to pose a serious threat to the life or health of any individual.[114]

---

112 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
113 *Freedom of Information Act 1982* (Cth) s 37(1).
114 Recs 29–2, 29–3.

Use of intermediaries

63.121 The IPPs do not provide expressly for the use of intermediaries to resolve situations in which access to information is denied by an agency under the *Privacy Act*. A consumer denied access to health information, however, could lodge a complaint with the Privacy Commissioner under s 36 of the Act. The FOI Act provides that where an agency denies a request for access to a document containing personal information provided by a 'qualified person', on the basis that disclosure of the information might be detrimental to the applicant's physical or mental health or wellbeing, the agency may provide the document to a 'qualified person' nominated by the applicant.[115]

63.122 In relation to organisations, NPP 6.3 sets out a process involving the use of intermediaries to assist in situations in which access is denied.

> If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

63.123 The OPC Review noted that this mechanism is very limited.[116] Organisations are only required to consider whether the use of an intermediary would meet the needs of the parties but are not required to take any further action.

63.124 There is a more stringent right to the use of an intermediary in the draft *National Health Privacy Code* where access to health information is refused on the ground that providing access would pose a serious threat to the life or health of the individual. A health service provider may offer to discuss information with the consumer, or nominate a suitably qualified health service provider to discuss the information with the individual. If this does not occur, or the health consumer is not satisfied with the process, the health consumer may nominate a health service provider to act as intermediary.

63.125 Once an intermediary has been appointed, the health service provider must provide the intermediary with the individual's health information. The intermediary may then consider, among other things, the validity of the refusal to grant access and, if he or she thinks it appropriate to do so, discuss the content of the health information with the individual.[117]

---

115 *Freedom of Information Act 1982* (Cth) s 41.

116 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 117.

117 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 5 div 3.

63.126 In IP 31, the ALRC asked whether the provisions of the draft *National Health Privacy Code* established a more appropriate and effective framework for providing access to health information than the *Privacy Act*.[118]

Submissions and consultations

63.127 The ANF expressed the view that:

> There remains significant resistance across the health system in granting access to health consumers to their personal health information that will require major culture change. Whether it is in relation to fear of revealing litigable conduct or health professional censure; or is part of the characteristic paternalism that is linked to benevolence that has been a feature of the provision of health services over many years, is neither here nor there. It does, however indicate that there needs to be significant efforts made to inform and actively assist that culture to change.[119]

63.128 Although the OPC was generally of the view that the provisions in the draft *National Health Privacy Code* dealing with access to health information were overly complex and prescriptive, the Office did express support for stronger provisions around the use of intermediaries to assist with access to health information.[120]

63.129 The NHMRC also expressed support for amending the *Privacy Act* to provide a more explicit right to the use of an intermediary.[121]

Discussion Paper proposals

63.130 In DP 72, the ALRC proposed that the 'Access and Correction' principle should provide stronger provisions on the use of intermediaries than the existing provisions in NPP 6.3. The proposed principle required organisations to take reasonable steps to reach a compromise involving the use of a mutually agreed intermediary, rather than simply requiring the organisation to consider the use of a mutually agreed intermediary.[122] The ALRC proposed that the OPC should provide guidance about what would amount to 'reasonable steps' in this context.[123] The ALRC also expressed the preliminary view that this provision would be useful in the context of providing access to personal information held by agencies, and, should apply to agencies.[124]

63.131 In addition, in relation to health information, the ALRC proposed more stringent requirements for the use of intermediaries in certain circumstances. The ALRC noted that almost half of the complaints lodged with the OPC against health service providers were in relation to access to health information, and that there

---

118 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–21.
119 Australian Nursing Federation, *Submission PR 205*, 22 February 2007.
120 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
121 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
122 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 26–2.
123 Ibid, Proposal 26–2.
124 Ibid, Proposal 12–8(c).

appeared to be some resistance among health service providers to allowing health consumers access to their health information. In the ALRC's view, this situation would improve if health service providers were required to refer the requested health information to a registered medical practitioner for a second opinion in relation to the question of access.

63.132 The proposed provisions—to be included in the new *Privacy (Health Information) Regulations*—stated that where an organisation denied an individual access to his or her own health information on the ground that providing access would be reasonably likely to pose a serious threat to the life or health of any individual, the organisation was required to advise the individual that he or she could nominate a registered medical practitioner to be given access to the health information. Once the individual had nominated a registered medical practitioner, the organisation would be required to provide the medical practitioner with access to the individual's health information. The medical practitioner would then assess the grounds for denying access to the health information and could provide the individual with access to the information if he or she was satisfied that to do so would not be likely to pose a serious threat to the life or health of any individual.[125]

63.133 The proposed regulation did not require that the nominated medical practitioner be mutually agreed upon. The ALRC asked whether an organisation should have the opportunity to object to the individual's choice of nominated medical practitioner before providing access to the individual's health information.[126]

Submissions and consultations

63.134 A number of stakeholders supported the proposed intermediary provisions.[127] The Victorian Office of the Health Services Commissioner expressed support for the provisions, but suggested that any such intermediary should be 'a suitably qualified health service provider', rather than a 'registered medical practitioner'.[128] The NHMRC also suggested that the intermediary might need to be a health care professional other than a medical practitioner.[129] The OPC was of the view that:

> In some circumstances, an appropriate intermediary might be a person that is not registered by a medical board, but who has sufficient clinical knowledge of a condition, as well as the individual's circumstances, to adequately and appropriately

125 Ibid, Proposal 57–6.
126 Ibid, [57.177].
127 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
128 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.
129 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

> serve in that role. For example, a counsellor in a support group for a specific condition might be a suitable intermediary.[130]

63.135 The OPC stated that the Office could develop guidance on what amounted to a suitable intermediary.[131] The Victorian Office of the Health Services Commissioner also suggested that the health service provider be required to provide the intermediary with the health information within a set period—suggesting 14 days would be appropriate—and that there was a need to address the question of fees.[132] Medicare Australia suggested that there should be an avenue of review available where there were concerns about the assessment made by the nominated medical practitioner.[133]

63.136 A number of stakeholders stated that the nominated medical practitioner should be mutually agreed upon and, in the event of a disagreement, that the Privacy Commissioner or another body should be given power to nominate an intermediary.[134] Avant Mutual Group Ltd stated that a provision along these lines was necessary to ensure that a medical practitioner with appropriate expertise was involved as an intermediary.[135] The OPC suggested that:

> If a provider did not reasonably believe that a nominated intermediary was appropriate in the circumstances, then it could refuse to provide access through the intermediary mechanism. In such a case, the individual could nominate an alternative intermediary, or have the option to complain to the Office. In assessing such a complaint, the Office would ask the provider to provide its reasons as to why the nominated intermediary was not appropriate. The Office would determine the merits of the provider's assessment of the nominated intermediary and whether there were valid grounds to deny allowing the individual to use that nominee as an intermediary. In many instances, the Office would likely seek expert clinical advice in resolving such disputes.[136]

63.137 Other stakeholders did not think that the nominated intermediary had to be mutually agreed upon.[137] The Victorian Office of the Health Services Commissioner, for example, was concerned that:

> If there was an opportunity for the organisation to object to a nominated practitioner who was agreeable to performing the role, then there would be little prospect of the consumer finding another practitioner who was willing to assume the role. Therefore the HSC does not support allowing an organisation to object to the individual's choice

---

130 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
131 Ibid.
132 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.
133 Medicare Australia, *Submission PR 534*, 21 December 2007.
134 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
135 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.
136 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
137 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.

of nominated practitioner, provided the intermediary is registered with the same registration board.[138]

ALRC's view

63.138 In Chapter 29, the ALRC considers the general right of access to personal information provided by the 'Access and Correction' principle. The ALRC recommends that the principle should provide that, where an agency or organisation is not required to provide an individual with access to his or her personal information, the agency or organisation must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.[139] This provision should apply to both agencies and organisations.

63.139 The more stringent intermediary provisions, dealing with denial of access to health information, should apply to both agencies and organisations. The provisions operate in limited circumstances where access to health information is denied on the basis that, in the case of an agency, providing access would, or could reasonably be expected to, endanger the life or physical safety of any person and, in the case of an organisation, providing access would be reasonably likely to pose a serious threat to the life or health of any individual. This formulation is based on the relevant exceptions in the FOI Act and the 'Access and Correction' principle.

63.140 The ALRC accepts that the proposal to allow only a 'registered medical practitioner' to act as an intermediary was too narrow. The recommendation has been amended to allow any suitably qualified health service provider to play this role. The ALRC notes that the OPC has offered to provide guidance on the qualifications necessary to fulfil this role. The ALRC has also provided a mechanism to resolve any dispute over the nomination of the intermediary. If an agency or organisation objects to the nominated health service provider and continues to refuse to provide access to the information, the individual may nominate another suitably qualified health service provider, or may lodge a complaint with the Privacy Commissioner. This provision is intended to allow the Privacy Commissioner to resolve those situations in which agreement cannot be reached.

63.141 The regulation recommended below is intended to operate in addition to the other provisions of the 'Access and Correction' principle. It is unnecessary, therefore, to address the issue of fees in the regulation as this matter is addressed in other provisions of the 'Access and Correction' principle.

---

138 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.
139 Rec 29–4.

Recommendation 63–6 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, if an individual is denied access to his or her own health information by an agency on the basis that providing access would, or could reasonably be expected to, endanger the life or physical safety of any person, or by an organisation on the basis that providing access would be reasonably likely to pose a serious threat to the life or health of any individual:

(a) the agency or organisation must advise the individual that he or she may nominate a suitably qualified health service provider ('nominated health service provider') to be given access to the health information;

(b) the individual may nominate a health service provider and request that the agency or organisation provide the nominated health service provider with access to the information;

(c) if the agency or organisation does not object to the nominated health service provider, it must provide the nominated health service provider with access to the health information within a reasonable period of time; and

(d) the nominated health service provider may assess the grounds for denying access to the health information and may provide the individual with access to the information to the extent that the nominated health service provider is satisfied that to do so, in the case of an agency, would not, or could not be reasonably expected to, endanger the life or physical safety of any person and, in the case of an organisation, would not be reasonably likely to pose a serious threat to the life or health of any individual.

If the agency or organisation objects to the nominated health service provider and refuses to provide the nominated health service provider with access to the information, the individual may nominate another suitably qualified health service provider, or may lodge a complaint with the Privacy Commissioner alleging an interference with privacy.

Health service is sold, transferred or closed

63.142 The OPC Review also considered the issue of access to personal health information where an organisation providing health services is sold or ceases to operate; for example, where a medical practitioner dies or retires or a practice closes.[140] In some jurisdictions, specific provision is made for the retention of medical records in

140 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 123.

these circumstances. In New South Wales, for example, outgoing medical practitioners must make reasonable efforts to ensure that medical records are kept by the medical practitioner taking over the practice or that they are provided to the patient to whom they relate.[141]

63.143 In Victoria, HPP 10 imposes express obligations on health service providers when the organisation providing the health service is to be sold, transferred or closed. These obligations include advertising in local newspapers indicating that the organisation is to be sold, transferred or closed and what the organisation proposes to do with the health information it holds.[142]

63.144 The draft *National Health Privacy Code* includes detailed provisions for dealing with health information on the transfer or closure of the practice of a health service provider. NHPP 10 requires health service providers to take reasonable steps to let health consumers know about the transfer or closure and to inform consumers about the proposed arrangements for the transfer or storage of consumers' health information.

63.145 The OPC Review noted that where a health service ceases to operate, this may raise issues relating to data security under NPP 4. There is a risk that 'abandoned' records may not be afforded adequate levels of storage and security.[143] It is also important to ensure that health information is available to health consumers seeking health services in the future.

63.146 The OPC considered that this was an important issue that should be addressed and made the following recommendations:

> The Australian Government should consider adopting the AHMAC code as a schedule to the *Privacy Act*. This will address the issue of access to health records when a health service ceases to operate. …
>
> The Australian Government should consider, if the AHMAC Code is not adopted into the *Privacy Act*, amending the NPPs to include a new principle along the lines of National Health Privacy Principle 10 in the AHMAC Code.[144]

63.147 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to deal with the situation in which a health service provider ceases to operate and whether NHPP 10 of the draft *National Health Privacy Code* provided an appropriate and effective framework.[145]

---

141 *Medical Practice Regulation 2003* (NSW) reg 8.
142 *Health Records Act 2001* (Vic) s 19, HPP 10.
143 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 123.
144 Ibid, rec 36.
145 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–22.

Submissions and consultations

63.148 The Victorian Office of the Health Services Commissioner supported a provision dealing expressly with the transfer or closure of health service practices and noted that:

> Distressed consumers have contacted [the Health Services Commissioner] advising they rang their doctor to find they had closed their practice and left no forwarding contact number. Some consumers have advised [the Health Services Commissioner] they last saw their doctor two or three weeks earlier, and had no notice of the closure.[146]

63.149 The OPC reiterated its view that:

> Amendment to the *Privacy Act* to introduce a privacy principle with a similar purpose as NHPP 10, would usefully clarify the obligations of health service providers and establish reasonable expectations for individuals on the handling of their health information in these circumstances.[147]

63.150 The NHMRC stated that:

> We strongly endorse the provisions in the draft *National Health Privacy Code* which address the management of health information on the transfer or closure of the practice of a health service provider. We understand that consumers are particularly concerned about the privacy of their health information when health care practices are acquired by larger corporate providers.
>
> We consider that maintenance of health care records is vital for the future quality health care of individuals and we also are cognisant of the risk to security of records if they are 'abandoned'.[148]

63.151 Other stakeholders agreed that the provisions of NHPP 10 dealing with the transfer or closure of a health service practice would be a useful addition to the *Privacy Act*.[149]

Discussion Paper proposal

63.152 In DP 72, the ALRC proposed that where a health service practice or business is sold, amalgamated or closed down and a health service provider will not be providing health services in the new practice or business, or the provider dies, the provider, or the legal representative of the provider, should be required to take all reasonable and appropriate steps to:

(a) make individual users of the health service aware of the sale, amalgamation or closure of the health service or the death of the health service provider; and

---

146 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.
147 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
148 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
149 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

(b) inform them about proposed arrangements for the transfer or storage of individuals' health information.

Submissions and consultations

63.153 In its submission to DP 72, the AMA acknowledged the importance of ensuring that health information is handled correctly when a health service closes, is sold or amalgamated, or when a health service provider dies. The AMA was aware that some health consumers had experienced difficulties accessing records in these circumstances and had issued guidance:

> The AMA *Privacy Handbook* states that where a practitioner retires and another doctor takes over the responsibility for the patient's records, it is appropriate for a circular to be sent out notifying patients of the doctor's retirement and advising that the nominated doctor in the practice will hold the records. If this is not feasible then the AMA considers it appropriate for the practice to inform the patient and provide the patient with the opportunity of having the records transferred to another doctor.
>
> The AMA also advises medical practitioners that if no arrangements can be made to transfer the records to another doctor, then suitable arrangements should be made so that they can be easily accessed if required and steps taken to ensure that patients are informed of the new arrangements.[150]

63.154 The AMA noted, however, that it might be logistically impossible to contact all health consumers, particularly where the practice involved is small, with limited resources. The AMA emphasised the importance of including the 'all reasonable and appropriate steps' element of the proposal.[151] Avant Mutual Group Ltd did not support this proposal, stating that, in the absence of evidence that there was a real problem in this area, it would impose an unjustified administrative burden on health service providers and their legal representatives.[152]

63.155 Dr Kerry Breen submitted that specialists often see health consumers on only one or two occasions. Detailed health information, including the specialist's assessment, investigation and opinion, is provided to the health consumer or referring health service provider. In these circumstances, Dr Breen was of the view that the obligation to contact health consumers should be limited to those seen in the previous twelve months, or likely to attend again. Dr Breen also suggested contacting all health service providers that had made a referral to the specialist in the last twelve months. In addition, a specialist might place an ad in the relevant state or territory AMA newsletter announcing the specialist's retirement and contact details for health

---

150 Australian Medical Association, *Submission PR 524*, 21 December 2007.
151 Ibid.
152 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

information. Dr Breen noted the importance of drawing a distinction between current and past patients.[153]

63.156 A number of other stakeholders also supported this proposal.[154] The Victorian Office of the Health Services Commissioner suggested, however, that the provision should be more prescriptive and provide greater guidance on what are reasonable and appropriate steps.[155] The NHMRC submitted:

> We consider that simply placing an advertisement in a locally-circulating newspaper is unlikely to constitute effective notification of many consumers, particularly if a practice is to be closed. We prefer the NSW approach which requires outgoing medical practitioners to make reasonable efforts to ensure that medical records are kept by the medical practitioner taking over the practice or that they are provided to the patient to whom they relate. We suggest that further guidance be given as to the steps that would be reasonable in different circumstances.[156]

63.157 The OPC stated that:

> The ALRC may wish to consider whether, in the interests of consistency, a test of 'reasonable steps' provides an appropriate threshold for these provisions, compared with 'all reasonable and appropriate steps'.[157]

ALRC's view

63.158 The ALRC recognises the importance of ensuring that health information is handled appropriately when a health service is sold, amalgamated or closed, or a health service provider dies. Health consumers should be notified when an event of this nature occurs so that they continue to have access to their information and the information is not lost or left with insufficient protection.

63.159 The regulation recommended below is based on NHPP 10 and requires health service providers, or their legal representatives, to take reasonable steps to ensure that individuals are aware of the sale, amalgamation or closure of the health service, or the death of the health service provider, and that they are informed about the proposed arrangements for the transfer or storage of their health information. In line with the ALRC's preference for principles-based regulation,[158] the ALRC has not included detailed rules about how this might occur—what amounts to 'reasonable steps' will depend on the circumstances of each case.

---

153 K Breen, *Submission PR 578*, 13 March 2008.

154 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

155 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.

156 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

157 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

158 See Ch 4.

63.160 The ALRC has adopted the 'reasonable steps' test because it provides an appropriate framework within which to ensure that health consumers are kept informed of what has happened to their health information, while recognising that, in some circumstances, it may not be possible to make contact with all individuals who have had dealings with a particular health service provider. It is also consistent with language used in other principles including the 'Access and Correction' principle, the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle and the 'Openness' principle.

Recommendation 63–7 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Data Security' principle, where an agency or organisation that provides a health service is sold, amalgamated or closed down, and an individual health service provider will not be providing health services in the new agency or organisation, or an individual health service provider dies, the provider, or the legal representative of the provider, must take reasonable steps to:

(a) make individual users of the health service aware of the sale, amalgamation or closure of the health service, or the death of the health service provider; and

(b) inform individual users of the health service about proposed arrangements for the transfer or storage of individuals' health information.

Health consumer changes health service provider

63.161 The *Privacy Act* does not deal specifically with the transfer of health information when a consumer changes health service providers. In Victoria, HPP 11 in the *Health Records Act* imposes an obligation on health service providers to provide 'a copy or written summary of the individual's health information' to another provider, if requested to do so by the individual or by the new provider on behalf of the individual. NHPP 11 of the draft *National Health Privacy Code* is in similar terms. Providing a mechanism of this sort ensures that the new health service provider has access to the health consumer's health information history.

63.162 The OPC Review recommended that the NPPs be amended to include a new principle along the lines of NHPP 11.[159]

159 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 34.

Submissions and consultations

63.163 The Victorian Office of the Health Services Commissioner noted that:

> Situations often occur where a medical practitioner or other health provider leaves a practice and their patients or clients follow them to their new practice. This can sometimes result in hundreds of requests for transfer of records made to the provider's old practice, and hostility between the two practices can emerge. [The Health Services Commissioner] attempts to assist providers to deal with these situations, and sometimes negotiates between two practices to resolve difficulties that arise. Therefore specific provisions in relation to the transfer of health information are very important and assist in the continuity of care of the health consumer.[160]

63.164 The OPC submitted that introducing a provision into the *Privacy Act* along the lines of NHPP 11 would be appropriate, as it would meet community expectations and would be consistent with good clinical care and continuity of treatment.[161] The NHMRC and other stakeholders also expressed support for including a provision in the *Privacy Act* dealing with the transfer of health information from one health service provider to another.[162]

63.165 DOHA agreed, noting that:

> The transfer of information from one health service provider to another, where an individual changes provider, is an important issue in the healthcare sector. It is consistent with good professional practice for a health service provider to respond positively to an individual's request to supply the individual's new provider with their original records (or a copy) or with a summary of the information in their records. This practice facilitates the continued availability of important health information when an individual changes health service provider, subject to the choices the individual exercises, thereby helping to ensure safe and effective healthcare for the individual.[163]

Discussion Paper proposal

63.166 In DP 72, the ALRC proposed that health service providers be required to transfer the individual's health information to another health service provider when requested to do so by the individual, or when requested to do so by the other health service provider acting with the authority of the individual. The health information could be provided in summary form.[164]

Submissions and consultations

63.167 A number of stakeholders expressed support for the ALRC's proposal in relation to the transfer of health information from one health service provider to

---

160 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.
161 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
162 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
163 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.
164 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 57–8.

another.[165] The AMA stated that it encourages doctors to follow best clinical practice and relevant codes of ethics to ensure that all medical records required by a new practitioner are provided.[166]

63.168 Some stakeholders were of the view that the provision should deal expressly or in more detail with issues such as: the evidence required of health consumer consent to transfer; recovering the costs of such transfers; the content and form of the records to be transferred; and the timeframe within which they should be transferred.[167] Dr Breen stated that:

> The biggest issues for patients wanting to have their records transferred are the attitude of the practice staff and the doctor (some of whom seem to take offence at any such request) and the fees charged. Unfortunately the AMA advice regarding fees for this service can be readily interpreted as 'open slather' and some fees are thus set as an obstacle. I suggest that consideration be given to advice about what constitutes a reasonable fee. Perhaps the ALRC could even suggest that Medical Boards inform the medical profession that actions designed to obstruct the ready transfer of health information upon request will be deemed to be unprofessional conduct?[168]

63.169 PIAC did not agree with the proposal that the health information could be provided in summary form.[169] The OPC suggested that

> greater specificity could be provided around the ability to transfer the information 'in summary form'. In the Office's view, it is important that a summarised version contains sufficient detail from the original records to be of assistance to the patient and provider. The ALRC and Australian Government may wish to consider whether the proposed provision on transfer of records should provide for relevant exceptions (similar to NPP 6.1), and requirements around permissible charges (similar to NPP 6.4).[170]

ALRC's view

63.170 Difficulties can arise in relation to the transfer of health information from one health service provider to another when a health consumer changes provider. Health consumers should have a right to have their health information transferred in these circumstances in a manner that ensures continuity of care. The new *Privacy (Health*

---

165 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

166 Australian Medical Association, *Submission PR 524*, 21 December 2007.

167 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

168 K Breen, *Submission PR 578*, 13 March 2008.

169 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

170 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

Information) Regulations should provide that, in addition to the other elements of the 'Access and Correction' principle, where an individual requests that his or her health information be transferred from one health service provider to another, the information must be transferred.

63.171 The regulation recommended below does not refer expressly to the situation in which an individual asks a health service provider to make the request on his or her behalf. Although the request is being made through the health service provider, the individual is still the requesting party. Ensuring valid consent will depend on the circumstances of the case. Where the request comes to the original health service provider from the new health service provider, for example, a signed consent to transfer may be appropriate. Where the request is made in person by the health consumer to the original health service provider, there may be no need to have anything in writing indicating consent.

63.172 The ALRC notes the OPC's suggestion that the requirement to transfer health information should be subject to exceptions similar to those currently set out in NPP 6.1 relating to access to personal information. The ALRC's intention is that the regulation recommended below will operate as part of, and in addition to, the other elements of the 'Access and Correction' principle. All the exceptions in that principle should apply to a request to transfer health information to a new provider, with any necessary amendments—for example, where the principle refers to 'providing access to information' it will need to be amended to refer to 'transferring the information'.

63.173 Requiring a health service provider to transfer health information to another health service provider can raise similar issues to providing the individual personally with access to the information. For example, the original health service provider may not be able to transfer the information, or may not wish to transfer the information, because the information relates to existing or anticipated legal proceedings between the health service provider and the individual, and the information would not be accessible by the process of discovery in those proceedings.[171]

63.174 In addition, the health service provider may consider that: the individual should not be provided with access to the information because this would be reasonably likely to pose a serious threat to the life or health of the individual; and that the health service provider the individual has nominated for transfer is unlikely to handle the information appropriately. In these circumstances, the original health service provider may wish to take advantage of the exception in the 'Access and Correction' principle that 'providing access would be reasonably likely to pose a serious threat to the life or health of any individual' and the new intermediary provisions recommended above.

---

171 This exception is set out in NPP 6.1(e) and is included in the 'Access and Correction' principle.

63.175 Other elements of the 'Access and Correction' principle will also apply to transfer between health service providers. For example, if an organisation charges to transfer the information, the charges may not be excessive and must not apply to lodging a request for transfer. In addition, the provision in the 'Access and Correction' principle requiring that information be provided in the manner requested by the individual, where reasonable and practicable, should apply to the transfer of health information. This general statement allows scope for health information to be transferred in summary form, if all the parties to the arrangement agree. Where it is not reasonable and practicable to transfer the information in the manner requested by the individual, it will not be necessary to do so.

Recommendation 63–8 (a) The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, where an individual requests that an agency or organisation that is a health service provider transfers the individual's health information to another health service provider, the agency or organisation must respond within a reasonable time and transfer the information.

(b) Other elements of the 'Access and Correction' principle relating to access should apply to a request for transfer from one health service provider to another, amended as necessary.

Management, funding and monitoring of health services

63.176 In its submission to the OPC Review, the NHMRC stated that health information was important in three areas: the provision of health services; management activities related to the provision of health services; and the conduct of research. The NHMRC noted that management activities include, for example: quality assurance; quality improvement; policy development; planning; evaluation; and cost-benefit analysis:

> The availability of health information without consent for quality assurance, research, and related activities is crucial to the safety and quality of clinical care, now and in the future. These activities, while similar in nature and intent, are currently subject to complex and different requirements under the *Privacy Act*, depending on the setting in which they are conducted and whether they are characterised as quality assurance or research.[172]

172 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

63.177 The OPC has issued guidance on the use and disclosure of health information for management, funding and monitoring activities, noting that:

> Such activities are likely to include those reasonably necessary for the ordinary running of the health service, including activities that support the community's expectation that appropriately high standards of quality and safety will be maintained. These expectations may be underpinned by professional standards or legal obligations.[173]

Management, funding or monitoring of a health service under the NPPs

63.178 The NPPs go some way towards acknowledging the public interest in allowing the use of health information in the management activities of health service providers. NPP 10.3 allows the collection of health information without consent in limited circumstances for:

- research relevant to public health or public safety;
- the compilation or analysis of statistics relevant to public health or public safety; or
- the management, funding or monitoring of a health service.

63.179 Although there is some overlap across these three areas, this chapter focuses on the third—that is, the management, funding and monitoring of health services. (Research is discussed in detail in Chapters 64, 65 and 66). The compilation and analysis of statistics relevant to public health or public safety can be conducted for research purposes or for management, funding or monitoring purposes. The ALRC does not propose to deal with this issue separately on the basis that, where the compilation or analysis of statistics is done for the purposes of the management, funding or monitoring of a health service, the activity can be subsumed in the provisions dealing with management, funding and monitoring activity.

63.180 Under the NPPs, health information may be collected without consent for management, funding and monitoring activities in the following circumstances. An organisation must consider whether it could use de-identified information to achieve its purpose. If this is not possible, it must be impracticable for the organisation to seek the consent of all the individuals involved. Finally, the information must be collected:

- as required by law;
- in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

---

173 Office of the Privacy Commissioner, *Use and Disclosure of Health Information for Management, Funding and Monitoring of a Health Service*, Private Sector Information Sheet 23 (2008).

- in accordance with guidelines approved by the Privacy Commissioner under s 95A of the *Privacy Act*.[174]

As required by law

63.181 NPP 10.3(d)(i) allows for collection of health information without consent where the collection is required by law. The OPC notes, for example, that:

> A radiologist is required under section 23DS of the *Health Insurance Act* to produce records of diagnostic imaging services, if requested by the Chief Executive Office of Medicare Australia. Under regulation 20 of the *Health Insurance Regulations 1975*, the radiologist is required to provide the name of the individual to whom the imaging service was provided and the date of the service.[175]

63.182 The 'Collection' principle allows the collection of sensitive information, including health information, without consent where the collection is required or authorised by or under law.[176] The 'Use and Disclosure' principle permits the use and disclosure of personal information, including health information, without consent where the use or disclosure is required or authorised by or under law.[177] It is not necessary, therefore, to include these elements specifically in the provision dealing with collection, use and disclosure of health information without consent for the management, funding, or monitoring of a health service. Where collection, use or disclosure is required or authorised by or under law, for any purpose, it is permissible under the relevant principles.

In accordance with rules on professional confidentiality

63.183 NPP 10.2 also allows the collection of health information for management, funding and monitoring of a health service when it is done in accordance with 'rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation'. The OPC indicated that it was not aware of any existing binding rules in the health sector that would meet these criteria.[178]

In accordance with s 95A Guidelines

63.184 Section 95A of the *Privacy Act* authorises the Privacy Commissioner to approve guidelines issued by the NHMRC in relation to the collection of health information for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety or the management, funding or monitoring of a health service. Section 95A also allows the Privacy Commissioner to approve

---

174 *Privacy Act 1988* (Cth) sch 3, NPP 10.3.

175 Office of the Privacy Commissioner, *Use and Disclosure of Health Information for Management, Funding and Monitoring of a Health Service*, Private Sector Information Sheet 23 (2008).

176 See Ch 21.

177 See Ch 25.

178 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

guidelines on the use and disclosure of health information under NPP 2.1(d)(ii) for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety. NPP 2 does not refer specifically to management, funding and monitoring of a health service. Before approving any such guidelines, the Privacy Commissioner must be satisfied that the public interest in the collection, use or disclosure of health information without consent for these purposes substantially outweighs the public interest in maintaining the level of privacy protection afforded by the NPPs.[179]

63.185 Currently, the Section 95A Guidelines require Human Research Ethics Committee (HREC) approval for management, funding or monitoring activities based on NPP 10.3(d)(iii). The NHMRC has noted that it is often difficult to distinguish management activities, such as quality assurance, from research in the health services context. It is of the view that, where such activities amount to research, they should always be conducted in accordance with the Section 95A Guidelines and be subject to review by an HREC.[180] For example, a hospital may collect information about surgical mortality rates for quality assurance purposes, but that information may also form the basis of a research project by hospital staff or others. The NHMRC has published some guidance on how to make the distinction between quality assurance activities and research, but suggests that even in relation to quality assurance activities that 'could infringe ethical principles that guide human research, independent ethical scrutiny of such proposals should be sought.'[181]

63.186 As noted above, while NPP 10 expressly provides for the collection of health information for management, funding or monitoring of a health service, NPP 2 does not expressly provide for the use or disclosure of health information for the same purpose. NPP 2 does allow, however, for the use and disclosure of health information without consent for a purpose directly related to the primary purpose for which the information was collected where the person would reasonably expect the organisation to use or disclose the information for that purpose.

63.187 The OPC Review stated that disclosure of health information for management activities generally would be within the reasonable expectations of individuals.[182] In response to concerns that the position is not clear, however, the OPC Review recommended that the OPC issue guidance to clarify when organisations can disclose

---

179 The current guidelines were issued in 2001: National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001) (the Section 95A Guidelines).

180 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

181 National Health and Medical Research Council, *When Does Quality Assurance in Health Care Require Independent Ethical Review?* (2003), 3. For the purposes of this Report, it is necessary to distinguish between the need for compliance with privacy legislation and the need for ethical review. Ethical review may include an analysis of privacy and confidentiality issues but is also concerned with the welfare and other rights of participants.

182 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

health information for the management, funding and monitoring of a health service.[183] The OPC subsequently issued an Information Sheet, which stated that:

> While health information will generally be collected by health service providers to afford treatment to patients, some health service management activities will be directly related purposes … Health service management activities that may be directly related purposes include service-monitoring, funding, complaint-handling, planning, evaluation and accreditation activities.
>
> They may also include disclosures to a medical expert for medico-legal opinion, an insurer, a medical defence organisation, or lawyer, solely for the purpose of addressing liability indemnity arrangements, for example, in reporting an adverse incident.
>
> Marketing, fund-raising, or research are unlikely to be directly related purposes, and generally consent should be obtained. In addition, training that does not relate to the direct provision of health care is also unlikely to be directly related and consent should be sought.[184]

63.188 In relation to 'reasonable expectations', the OPC noted that:

> A patient's expectations can be effectively managed through good provider-patient communication. This usually means the patient has been told the use or disclosure would happen, or they would expect it to happen in the context of why they provided the information in the first place. If the patient would not reasonably expect the use or disclosure that the provider has in mind, such as for managing a health service, then the provider will usually need to get the patient's consent before proceeding.[185]

Management, funding or monitoring of a health service under the IPPs

63.189 Management activities are undertaken in both the public and the private health sectors. The IPPs, however, do not make specific reference to management, funding and monitoring activities and so it is necessary to interpret the basic principles to decide whether it is possible to use health information in the public sector for such activities.

63.190 The use of health information for management activities may involve collection, use or disclosure of the information. IPP 1 allows collection of health information so long as it is for a lawful purpose, directly related to the activities of the agency. IPP 1 does not require consent to collect personal information, including health information. This would seem to allow collection of health information by public sector health service providers for management, funding and monitoring activities directly related to the agency's activities.

---

183 Ibid, rec 61.

184 Office of the Privacy Commissioner, *Use and Disclosure of Health Information for Management, Funding and Monitoring of a Health Service*, Private Sector Information Sheet 23 (2008).

185 Ibid.

63.191 IPP 10 allows use of health information without consent for the primary purpose for which it was collected and any directly related secondary purpose. As noted above, the OPC is of the view that a range of management, funding and monitoring activities are directly related to the collection of health information in the context of providing a health service to an individual.

63.192 IPP 11 allows disclosure of health information without consent where the individual concerned is reasonably likely to have been aware that health information was usually disclosed to the particular person, body or agency. As noted above, the OPC considers that this issue can be addressed by reasonable provider-consumer communication.

State and territory legislation

63.193 Both the New South Wales *Health Records and Information Privacy Act* and the Victorian *Health Records Act* expressly provide for the use or disclosure of health information without consent in the public and private sectors for various management activities related to funding, planning, monitoring, improvement or evaluation of health services, and for training provided to employees or others working with the health services organisation.[186] Any such use or disclosure is subject to certain criteria; for example, it must be impracticable to seek individuals' consent and reasonable steps must be taken to de-identify the information. Use or disclosure of health information for management activities under these Acts does not depend on establishing that it is a directly related secondary purpose or that it would be within individuals' reasonable expectations.

Issues Paper 31

63.194 In IP 31, the ALRC asked whether guidance by the OPC to clarify that organisations can disclose health information for the management, funding and monitoring of a health service was an appropriate and effective response to the lack of clarity in this area.[187]

63.195 The NHMRC submitted that:

> The complexity of these provisions has not been resolved for NHMRC stakeholders by the guidance provided to date by the Office of the Privacy Commissioner, partly because of the restrictions imposed by the 'reasonable expectation' requirement on the circumstances in which health information can be used or disclosed for quality assurance and related activities, and partly because of the underlying inconsistencies in relation to disclosure on the one hand and collection on the other. Much greater clarity of the status of these important activities is required.[188]

---

186 *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 10; *Health Records Act 2001* (Vic) sch 1, HPP 2.2.

187 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–9.

188 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

63.196 Other major stakeholders also expressed the view that further guidance from the OPC would not be an adequate response to concerns. These stakeholders supported amending the *Privacy Act* to deal expressly with the collection, use and disclosure of health information for management activities.[189]

63.197 The NHMRC and the Australian Commission on Safety and Quality in Health Care (ACSQHC) suggested that collection, use and disclosure of health information without consent for management activities be allowed where it is conducted in accordance with guidelines issued by the Privacy Commissioner or, alternatively, a PID issued by the Privacy Commissioner. Both stakeholders also expressed the view that some of this activity could proceed legitimately without being subject to review by an HREC.[190] The ACSQHS also noted that, for most quality and safety indicators, a probabilistic matching process can be used, and individuals need not be uniquely identified.[191]

63.198 A final issue that was raised by the Australian Health Insurance Association (AHIA) concerned the use of health information to report on the charging practices and performance of health service providers.

> At present the National Privacy Principles (NPPs) are interpreted to mean that health funds must have the consent of practitioners to disclose their billing practices or information on the number and types of procedures and other services they perform. This can be regarded as business rather than personal information and it must be questioned whether this was the intended effect of the privacy laws and NPPs.[192]

63.199 The OPC has stated that if an individual's identity can be determined from business information, then the information is personal information for the purposes of the *Privacy Act*. Where this information is sensitive information, including health information, it generally must be collected with consent.[193]

63.200 The AHIA noted the following recommendations of the Taskforce on Reducing the Regulatory Burden on Business:

---

189 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

190 Australian Commission on Safety and Quality in Health Care, *Submission PR 252*, 14 March 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

191 Australian Commission on Safety and Quality in Health Care, *Submission PR 252*, 14 March 2007.

192 Australian Health Insurance Association, *Submission PR 161*, 31 January 2007.

193 Office of the Privacy Commissioner, *Frequently Asked Questions: When is Business Information Covered by the Privacy Act?* <www.privacy.gov.au/faqs/bf/q8.html> at 30 April 2008.

> The Australian Government should facilitate the publication of industry-wide data on the charging practices of individual medical specialists.[194]
>
> The Australian Government should amend laws to enable data on hospital treatment outcomes to be published.[195]

63.201 In August 2006, the Australian Government agreed in principle with these recommendations and undertook to improve the information available to health consumers. It made clear, however, that:

> Information about doctors' fees needs to be considered sensitively as it relates directly to the charging practices of medical specialists, and impacts directly on the interface between the medical provider and the consumer … [and] proposals to publish data on hospital treatment outcomes need to be considered sensitively as they relate to the clinical outcomes of decisions made by health care providers.[196]

63.202 Although the *Privacy Act* has an impact on the publication of this kind of information, the issue is not, primarily, a privacy issue. As noted in the Australian Government response to *Rethinking Regulation*, the publication of detailed information on the charging practices and performance of health service providers is likely to have industry-wide implications, and any proposed reform will need to take these into account. A detailed consideration of these issues falls outside the terms of reference for this Inquiry. While the *Privacy Act* would not stand in the way of this kind of regulatory reform, in the absence of such reform the *Privacy Act* will apply to such information.

Discussion Paper proposals

63.203 In DP 72, the ALRC proposed that the *Privacy (Health Information) Regulations* should make express provision for the collection, use and disclosure of health information without consent where necessary for the funding, management, planning, monitoring, improvement or evaluation of a health service. This would be allowed where:

- the purpose could not be achieved by the collection, use or disclosure of information that did not identify the individual;
- it was impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and

---

194 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), rec 4.11.

195 Ibid, rec 4.12.

196 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 5–6.

- the collection, use or disclosure was conducted in accordance with rules issued by the Privacy Commissioner.[197]

63.204 The ALRC also proposed that the *Privacy Act* be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, improvement or evaluation of a health service.[198]

63.205 The ALRC's proposals were premised on the existence of a clear public interest in allowing the collection, use and disclosure of health information for the funding, management, planning, monitoring, improvement or evaluation of health services in defined circumstances. In the ALRC's view, the public interest in allowing such activities to proceed outweighs the public interest in maintaining the level of privacy protection provided by the NPPs. The ALRC was not persuaded that individuals would be aware or expect that their health information was collected, used and disclosed without consent for such activities. It is important to allow such activities to proceed, whether or not they fall within individuals' reasonable expectations.

63.206 The ALRC adopted the more detailed description of management, funding and monitoring activities from provisions in the draft *National Health Privacy Code*, the New South Wales *Health Records and Information Privacy Act* and the Victorian *Health Records Act*—that is, funding, management, planning, monitoring, improvement or evaluation of health services—to make clear that health information can also be used to evaluate and improve the provision of health services.[199]

63.207 The proposed rules to be issued by the Privacy Commissioner were intended to replace the 'rules established by competent health or medical bodies that deal with obligations of professional confidentiality' required by NPP 10.3(d)(ii) and the guidelines—issued by the NHMRC and approved by the Privacy Commissioner under s 95A of the *Privacy Act*—required by NPP 10.3(d)(iii).

63.208 The ALRC noted that some funding, management, planning, monitoring, improvement and evaluation activities also may be characterised as research. Where particular activities can be characterised as both management activities and research, the ALRC expressed the view that the activity should be conducted in accordance with the proposed rules issued by the Privacy Commissioner in relation to management activities and should also be subject to the provisions relating to research, discussed in Chapters 64–66.

---

197 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 57–9.
198 Ibid, Proposal 57–10.
199 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 2.2(f)(i).

63.209 The New South Wales and Victorian health privacy legislation and the draft *National Health Privacy Code* allow the use of health information without consent for training purposes in some circumstances.[200] The ALRC expressed the view that the public interest balance in relation to training activities is not the same as the public interest balance in ensuring the quality and safety of health care. Health information used in the training context should be used in accordance with the proposed UPPs; and special provision should not be made for this activity.

Submissions and consultations

63.210 The AMA submitted that allowing the collection, use and disclosure of health information without consent for the funding, management, planning, monitoring, improvement or evaluation of a health service was a very broad exception, and had the potential to affect the relationship of trust and confidentiality between health service providers and consumers. The AMA also expressed concern about the use of the term 'impracticable' in relation to 'impracticable to seek consent', and asked whether this would include mere inconvenience or cost.[201]

63.211 The NHMRC also expressed concern about the use of the term 'impracticable':

> We note, however, that in some circumstances a consent requirement which may result in less than full access to relevant records is likely to damage the validity of a quality assurance project or program. We are concerned that potential damage to the validity of a project or program by seeking consent may not be interpreted consistently as an issue of 'impracticality'; in such circumstances seeking consent may be viewed as 'practicable' in the sense that subjects are easily contactable, thereby precluding the relevant collection despite the project or program being in the overall public interest.[202]

63.212 The Australian Privacy Foundation, on the other hand, expressed support for the proposal, noting that it set a high threshold for use of health information without consent for management purposes:

> As noted earlier, it is all too easy for agencies and organisations to assert a need for collection, use and disclosure of personal information on grounds of administrative convenience or efficiency. Particularly in the case of health information, it needs to be established that the use of personally identifiable information is necessary and that seeking consent is impracticable—not merely inconvenient or expensive.[203]

---

200 *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 10(1)(e); *Health Records Act 2001* (Vic) sch 1, HPP2.2(f)(ii); National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 2.2(f)(ii).

201 Australian Medical Association, *Submission PR 524*, 21 December 2007.

202 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

203 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

63.213 Other key stakeholders also expressed support for the proposal[204] and for the related proposal that the Privacy Commissioner be empowered to issue binding rules in relation to the use of health information in the funding, management, planning, monitoring, improvement or evaluation of a health service.[205] Privacy NSW was also supportive, noting that:

> In our view individuals would be unlikely to expect that their personal information will be collected, used or disclosed for funding, management, planning, monitoring, improvement or evaluation of health services. We therefore welcome the proposal that there be limitations placed on the collection, use or disclosure of health information for those purposes, and that the OPC be given the power to issue guidelines in relation to these matters.[206]

63.214 The OPC also supported the proposals in general terms, but indicated that the proposed rules should be issued by the NHMRC and approved by the Privacy Commissioner. In addition, the OPC was of the view the term 'improvement' was an unnecessary addition to the list of allowable activities.[207]

63.215 The Health Informatics Society of Australia suggested a number of other options in relation to such management activities. These included:

- a one-off review by an HREC of current and future management activities where the HREC would have to be satisfied that the policies and practices established provided sufficient privacy protection;
- an approval process that did not involve HRECs but was based on a clear definition of the activity as one intended to improve local service delivery;
- the development of guidelines by the NHMRC to provide adequate regulation.[208]

63.216 The OPC and other stakeholders agreed with the ALRC that the public interest balance in relation to training activities was not the same as the public interest balance in ensuring the quality and safety of health care, and that special provision should not

---

204 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

205 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

206 Privacy NSW, *Submission PR 468*, 14 December 2007.

207 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

208 Health Informatics Society of Australia, *Submission PR 554*, 2 January 2008.

be made for this activity.[209] A number of other stakeholders, however, did not agree, arguing that appropriately trained health service providers are fundamental to the delivery of high quality and safe health services.[210]

ALRC's view

63.217 Funding, management, planning, monitoring and evaluation of health services should be able to proceed in defined circumstances using individuals' health information without consent. The recommendation below makes clear that, generally, these activities can and should be conducted either on the basis of consent, or using health information that does not identify individuals. Identifiable health information may only be used where the purpose cannot be achieved using information that does not identify individuals. In addition, it must be unreasonable or impracticable to seek individuals' consent and any collection, use or disclosure must be conducted in accordance with binding rules issued by the Privacy Commissioner.

63.218 The ALRC has dropped the reference to 'improvement' of a health service, on the basis that this is subsumed in evaluation and planning activities.

63.219 The ALRC has modified the wording dealing with consent suggested in DP 72. The recommendation below requires that it be 'unreasonable or impracticable' rather than just 'impracticable' to seek consent. This acknowledges that, while it might be practicable to seek consent in terms of it being logistically possible, seeking consent may lead to an incomplete or biased sample due to self selection. It is important to ensure that the integrity and validity of management activities aimed at safety and quality in the health care sector are not compromised in this way.[211]

63.220 Since binding rules form part of the legal framework for handling health information without consent, these should be issued by the Privacy Commissioner. The rules could address issues such as: who may collect, use and disclose identified health information without consent for management activities; limits on further use and disclosure of the information; requirements to destroy information, and requirements to render health information non-identifiable before publication of any management papers or reports.

---

209 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

210 Confidential, *Submission PR 570*, 13 February 2008; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.

211 This issue is discussed in detail in relation to research results in Ch 65.

63.221 The NHMRC has noted that management activity that does not amount to research should not require review by an HREC.[212] The ALRC agrees with this view and has recommended that such activity should proceed simply in accordance with the management rules issued by the Privacy Commissioner.

63.222 The ALRC recognises, however, that some funding, management, planning, monitoring and evaluation activities may also be characterised as research. Where particular activities can be characterised as both management activities and research, the activity should be conducted in accordance with the management rules issued by the Privacy Commissioner and should also be subject to the provisions relating to research, discussed in Chapters 65 and 66. The research exceptions recommended in those chapters, like the Section 95 and 95A Guidelines, provide for review of research proposals by an HREC.

63.223 Finally, it is possible that, while not amounting to research, some management activity may still require ethical review. The NHMRC has provided guidance on when this might be necessary, for example, where a proposed quality assurance activity poses risks for, or imposes burdens on, health consumers beyond those of their routine care.[213] The ALRC notes this advice, although the broader issue of ethical review of management activities is outside the Inquiry's terms of reference.

63.224 The public interest balance in relation to training activities is not the same as the public interest balance in ensuring the quality and safety of health care. Health information used in the training context should be used in accordance with the UPPs and special provision should not be made for this activity.

63.225 Finally, health consumers should be made aware, as far as possible, that their health information may be used without consent for the funding, management, planning, monitoring, or evaluation of a health service.

Recommendation 63–9 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle and the 'Use and Disclosure' principle, an agency or organisation may collect, use or disclose health information where necessary for the funding, management, planning, monitoring, or evaluation of a health service where:

212 National Health and Medical Research Council, *When Does Quality Assurance in Health Care Require Independent Ethical Review?* (2003), 5.

213 Ibid, 6.

(a) the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual or from which the individual would not be reasonably identifiable;

(b) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and

(c) the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.

Recommendation 63–10 The *Privacy Act* should be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, or evaluation of a health service.

64. Research: Current Arrangements

Contents

Introduction

64.1 This chapter examines the special arrangements in place under the *Privacy Act 1988* (Cth) to allow for the use of personal information in health and medical research. The Act currently provides for the use of personal information—including health information—without consent, for health and medical research, where the research is conducted in accordance with guidelines issued by the National Health and Medical Research Council (NHMRC) and approved by the Privacy Commissioner. These arrangements recognise that, in some circumstances, the public interest in allowing particular research projects to proceed outweighs the public interest in maintaining the level of privacy protection provided by the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs).

64.2 These arrangements are currently limited to the use of personal information for medical research under the IPPs, and the use of health information for research, or the compilation or analysis of statistics, relevant to public health or public safety under the NPPs. The following chapter considers whether these arrangements should be extended to include the use of personal information in other sorts of research, in areas such as criminology and sociology.

Health and medical research in Australia

64.3 The Hon Tony Abbott MP, former Minister for Health and Ageing, noted in 2004 that:

> Australia is a world leader in health and medical research. On a per capita basis, our research output is twice the OECD average, even though we spend much less, per capita, than the UK or the USA.
>
> Investment in health and medical research makes good economic and health sense. It generates significant returns both in terms of health benefits—longevity and increased

> quality of life for Australian people generally; and economic benefits, through increased knowledge based jobs and economic activity.[1]

64.4 There is strong community support for health and medical research in Australia. In a survey conducted for Research Australia in 2007, 89% of participants thought that health and medical research was an industry important to Australia's future. Of survey participants, 85% considered that increased funding for health and medical research should be a priority for the Australian Government.[2]

64.5 In a joint submission to this Inquiry, the Cancer Council Australia and the Clinical Oncological Society of Australia noted that cancer accounts for more deaths in Australia than any other individual cause. One in two Australian men and one in three Australian women are expected to be diagnosed with cancer by the age of 85. The submission also noted that cancer survival in Australia has improved by 30% over the past two decades, in large part facilitated by breakthroughs in epidemiological, laboratory and clinical research.[3]

64.6 The NHMRC plays an important role in fostering health and medical research in Australia. The NHMRC is a statutory authority, within the portfolio of the Minister for Health and Ageing, established by the *National Health and Medical Research Council Act 1992* (Cth) (the NHMRC Act). The Act provides that the role of the NHMRC is to:

- raise the standard of individual and public health throughout Australia;
- foster the development of consistent health standards between the various states and territories;
- foster medical research and training and public health research and training throughout Australia; and
- foster consideration of ethical issues relating to health.[4]

64.7 The NHMRC is also the peak funding and advisory body for health and medical research in Australia and makes recommendations to the Minister for Health and Ageing on the funding of health and medical research and training. Australian Government funding of such research is provided primarily through grants from the Medical Research Endowment Account (MREA), established under the NHMRC Act.[5] The Australian Government has more than doubled investment in health and medical

---

1 Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle For a Healthy Competitive Australia* (2004), Minister's Forward.
2 Research Australia, *Health and Medical Research Public Opinion Poll 2007* (2007).
3 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007.
4 *National Health and Medical Research Council Act 1992* (Cth) s 3.
5 Ibid pt 7.

research since 1999.[6] Funding provided for the MREA was $430.4 million in 2005–06,[7] $627.2 million in 2006–07[8] and $530.3 million in 2007–08.[9] Some research funding also is provided through the Australian Research Council and other schemes.

64.8 In a 2004 report, the Investment Review of Health and Medical Research Committee estimated that, of the $1.7 billion invested in Australian health and medical research in 2000–01, 47% was provided by the Australian Government, 44% by the private sector and 9% by state and local government.[10]

64.9 The report noted that the bulk of Australian Government investment in this period was directed to the higher education sector, although some of this research was then performed by, or in conjunction with, other institutions. Smaller amounts were spent by the Australian Government directly through agencies such as the Department of Health and Ageing (DOHA) and the Commonwealth Scientific and Industrial Research Organization (CSIRO), or channelled to businesses or non-profit groups. State governments spent the bulk of their investment in their own institutions, including state departments of health, medical research institutes and public hospitals. The business sector largely funded its own research. The non-profit sector funded half of its research from its own fundraising, and the other half through investment from the Australian Government, state governments and business.[11]

64.10 The NHMRC noted in its submission to the Office of the Privacy Commissioner's (OPC) review of the private sector provisions of the *Privacy Act* (the OPC Review) that:

> Consistent with patterns of the provision of clinical care, the conduct of health and medical research in the Australian health care system frequently spans the public and private sectors.
>
> Much health and medical research is multi-site or multi-jurisdictional, involving participants who move between the public and private health sectors.[12]

---

6 National Health and Medical Research Council, *Role of the NHMRC* <www.nhmrc.gov.au/about/role/index.htm> at 25 March 2008.

7 Australian Government Department of Health and Ageing, *2005–06 Portfolio Budget Statements: Outcome 11 Health and Medical Research* (2005).

8 Australian Government Department of Health and Ageing, *2006–07 Portfolio Budget Statements: Outcome 14 Health and Medical Research* (2006).

9 Australian Government Department of Health and Ageing, *2007–08 Portfolio Budget Statements: National Health and Medical Research Council* (2007).

10 Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle For a Healthy Competitive Australia* (2004), 17.

11 Ibid, 17.

12 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

64.11 Under the NHMRC Act, the Australian Health Ethics Committee (AHEC)—a principal committee of the NHMRC—has responsibility for developing guidelines for the ethical conduct of medical research.[13] The primary set of guidelines for human research, developed jointly by the NHMRC, the Australian Research Council and the Australian Vice Chancellors' Committee (AVCC), is the 2007 *National Statement on Ethical Conduct in Human Research.*[14] This National Statement replaces the 1999 *National Statement on Ethical Conduct in Research Involving Humans* and was developed following extensive public consultation and debate.

64.12 The National Statement sets out ethical principles relevant to research involving humans and guidance on the formation, membership and functions of Human Research Ethics Committees (HRECs). It is important to note that, while the guidelines in the National Statement that are applicable to the conduct of health and medical research involving humans are issued by the NHMRC in fulfilment of its statutory obligations, the National Statement applies to *all* research involving humans, not only health and medical research.

64.13 The National Statement provides that any research proposals involving more than a low level of risk to participants must be reviewed and approved by an HREC. It also sets out requirements to be followed by:

- institutions or organisations in establishing HRECs;
- researchers in submitting research proposals to HRECs; and
- HRECs in considering and reaching decisions regarding research proposals and in monitoring the conduct of approved research.

64.14 The *Privacy Act* regime incorporates the HREC approval process established by the National Statement to ensure that where research is conducted using personal information without consent, that research is conducted with due regard for the balance of public interests and the protection of personal information.

64.15 Although the National Statement is not legally binding, the Statement stipulates that it must be used to inform the design, ethical review and conduct of human research that is funded by, or takes place under the auspices of, the NHMRC, the Australian Research Council or the AVCC. Compliance with the National Statement is a condition of NHMRC grants of research funding.[15] In addition, in order for an institution to apply to be an NHMRC Administering Institution for the purposes of applying for, and subsequently administering, NHMRC research funds, all research

---

13 *National Health and Medical Research Council Act 1992* (Cth) s 35(3).

14 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

15 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [14.1]–[14.8].

conducted within the institution—whether or not funded by the NHMRC—must comply with the National Statement.[16]

64.16 The power to withdraw funding is the most important and direct mechanism by which the NHMRC may induce compliance with the National Statement. As noted above, however, not all health and medical research is funded by the Australian Government on the advice of the NHMRC. The issue of enforcing compliance with the National Statement was considered in detail in *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96).[17] In that report, the ALRC and AHEC recommended that the NHMRC review the mechanisms for achieving compliance with the National Statement, with particular regard to human research conducted wholly within and funded by the private sector.[18]

64.17 The recommendations set out in the following chapters will ensure that any research—whether conducted in the public or the private sector and however it is funded—that is undertaken on the basis of the research exceptions in the *Privacy Act*, will have to be considered and approved by an HREC constituted in accordance with, and acting in compliance with, the National Statement.[19]

Research and the use of personal information

64.18 The conduct of health, medical and other human research frequently involves the collection and use of personal information about individuals. Generally, individuals who participate in research projects do so on the basis of consent and, in these circumstances, it is possible to handle participants' personal information in compliance with the IPPs or the NPPs. The National Statement makes clear that:

> Respect for human beings involves giving due scope to people's capacity to make their own decisions. In the research context, this normally requires that participation be the result of a choice made by participants—commonly known as 'the requirement for consent'. This requirement has the following conditions: consent should be a voluntary choice, and should be based on sufficient information and adequate understanding of both the proposed research and the implications of participation in it.[20]

64.19 The OPC Review noted that consumer research on attitudes in this area have produced mixed results. Research conducted by the OPC indicated that individuals

---

16 National Health and Medical Research Council, *Administering Institutions Policy*, 6.

17 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Ch 14.

18 Ibid, Rec 14–1.

19 See, in particular, Recs 65–9 and 65–10.

20 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), 19. The concept of consent under the *Privacy Act* is discussed in detail in Ch 19.

were concerned about their personal information being used, even in a de-identified form, for research purposes. Almost two thirds (64%) of respondents felt that consent should be obtained before de-identified information derived from personal information was used for research purposes. One third (33%) of respondents felt that permission was not necessary.[21]

64.20 The Australian Consumers' Association, in its submission to the OPC Review, expressed the view that when consumers go to the doctor, they provide health information on the basis that it will be used only for the purposes of their clinical care:

> They don't expect that third parties will be trawling through their health records; even if it is in de-identified form. In this sense third party access to data without the consumers' knowledge is something of a breach of trust.[22]

64.21 On the other hand, DOHA research suggests that, although consumers express reservations about identified personal information being made available for purposes other than their own clinical care, generally they are very accepting of the notion of sharing de-identified health information amongst health planners and researchers.[23] Research conducted by the NHMRC indicated that there was considerable support among the general public (66%) and health consumers (64%) for approved researchers to match information from different databases. There was an even higher level of support for approved researchers to access health information from databases where health information was identified by a unique number rather than a name.[24]

64.22 A 2005 survey of patients attending the Medical Oncology Outpatient Clinic at the Royal Adelaide Hospital indicated that 93% would allow their health information to be used for research, so long as it was kept confidential and they couldn't be identified. Where the health information could be identified, 32.8% would allow the information to be used without consent. A further 14.9% would allow the use of the information without consent if the project was approved by an HREC and a further 5.6% would allow the use of the information without consent if it was impracticable to obtain their consent.[25]

64.23 In their joint submission, the Cancer Council Australia and the Clinical Oncological Society of Australia suggested, in relation to these survey results, that the community would be even more supportive of the use of their health information if it had a better understanding of how such research could contribute to improvements in

---

21 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.

22 Australian Consumers Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 October 2004.

23 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

24 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

25 C Beeke, I Olver and K McLaughlin, 'A Survey of Patients' Attitudes Towards the Use of Their Health Data' (2007) 34(4) *Journal of Registry Management* 119.

cancer prevention, detection and treatment. These results were also likely to improve if the community was better informed about the mechanisms available to protect privacy.[26] A number of submissions to the OPC Review noted that the issue of community support could be addressed by greater efforts to increase public awareness and acceptance of the use of personal information for research, and in particular, epidemiological research.[27]

64.24 Both the National Statement and the *Privacy Act* recognise that in some circumstances it is very difficult or impossible to conduct research that may be in the public interest—for example, epidemiological studies of the distribution and determinants of disease in large populations—in a way that complies with the IPPs and the NPPs. As the CSIRO has noted:

> Informed consent and opt-in is a good model for clinical trials, for example, where the risk is normally predominantly to the participating individual. However, in the case of population health research, the findings will often be implemented for the whole population. In these cases informed consent and opt-in may not be good models because non-participation can introduce bias and therefore affect the applicability of the results.[28]

64.25 In a 2006 paper, the Academy of Medical Sciences in the United Kingdom canvassed the impact that consent requirements can have on research in some circumstances. Seeking consent to use personal information for research can lead to self-selection bias among research participants. The paper notes that non-response rates are high in 'hard to reach' populations—for example, certain ethnic groups and in areas of social disadvantage. This means that these groups are poorly represented in research results. On the other hand, one survey suggested that people from higher socio-economic groups, older adults and men tend to be more willing than other groups to give consent for researchers to use their health information. This can give rise to systemic errors in research results, through the introduction of bias in the study sample.[29]

---

26 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007.

27 Australasian Epidemiology Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004; Telethon Institute for Child Health Research, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

28 CSIRO, *Submission PR 176*, 6 February 2007.

29 Academy of Medical Sciences, *Personal Data for Public Good: Using Health Information in Medical Research* (2006), 59–61.

64.26 The Academy's paper also included the following case study:

> Until 2001, there was a great deal of controversy about a potential link between the termination of pregnancy and an increased risk of breast cancer. Several studies gave conflicting results. Most studies until this point involved interviews with patients. A much discussed issue at the time was whether such studies were subject to reporting bias, ie that women with breast cancer might be more likely than control women (with no history of breast cancer) to tell the interviewer if they had had a termination. Such bias would greatly reduce the accuracy and validity of the results.
>
> To circumvent potential reporting bias, researchers conducted a study based on linkage of independent records. Data were analysed from HNS hospital admissions and death certificates without consent. The analysis showed no increase in breast cancer risk after termination of pregnancy. This conclusive result ended the previous speculation and provided more accurate information for patients.[30]

64.27 The *Privacy Act* provides a mechanism to allow such research to go forward without consent, subject to guidelines issued by the NHMRC and approved by the Privacy Commissioner. The Act provides for two sets of binding guidelines in the area of health and medical research: one set of guidelines binding on public sector agencies made under s 95 of the Act, and one set of guidelines binding on private sector organisations made under s 95A. Sections 95 and 95A both require the Privacy Commissioner to be satisfied, before approving the guidelines, that the public interest in the relevant research outweighs to a substantial degree the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs.

Information Privacy Principles

64.28 The IPPs themselves do not refer to the use of personal information for health and medical research. Section 95 of the *Privacy Act*, however, provides as follows:

> (1) The CEO of the National Health and Medical Research Council may, with the approval of the Commissioner, issue guidelines for the protection of privacy in the conduct of medical research.
>
> (2) The Commissioner shall not approve the issue of guidelines unless he or she is satisfied that the public interest in the promotion of research of the kind to which the guidelines relate outweighs to a substantial degree the public interest in maintaining adherence to the Information Privacy Principles.
>
> (3) Guidelines shall be issued by being published in the *Gazette*.
>
> (4) Where:
>
> (a) but for this subsection, an act done by an agency would breach an Information Privacy Principle; and
>
> (b) the act is done in the course of medical research and in accordance with guidelines under subsection (1);
>
> the act shall be regarded as not breaching that Information Privacy Principle.

30 Ibid, 61.

> (5) Where the Commissioner refuses to approve the issue of guidelines under subsection (1), an application may be made to the Administrative Appeals Tribunal for review of the Commissioner's decision.

64.29 The current *Guidelines under Section 95 of the Privacy Act 1988*[31] (Section 95 Guidelines) were issued in 2000. Once these guidelines were approved by the Privacy Commissioner and published in the Australian Government *Gazette*, they gained the force of law. If an agency does an act in the course of medical research that would have breached the IPPs but is consistent with the Section 95 Guidelines, the act is regarded as not breaching the IPPs.

National Privacy Principles

64.30 The NPPs, unlike the IPPs, specifically provide for the use of health information in research. NPPs 2 and 10 provide that health information may be collected, used and disclosed where necessary for research or the compilation or analysis of statistics, relevant to public health or public safety where:

- the purpose cannot be served by the collection of information that does not identify the individual;[32]
- it is impracticable for the organisation to seek the individual's consent to the collection, use or disclosure;[33]
- the information is collected, used and disclosed in accordance with guidelines approved under s 95A;[34]
- in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information;[35] and
- the organisation takes reasonable steps to permanently de-identify the information before it discloses it.[36]

---

31 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000).
32 *Privacy Act 1988* (Cth) sch 3, NPP 10.3(b).
33 Ibid sch 3, NPPs 2.1(d)(i), 10.3(c).
34 Ibid sch 3, NPPs 2.1(d)(ii), 10.3(d).
35 Ibid sch 3, NPP 2.1(d)(iii).
36 Ibid sch 3, NPP 10.4.

64.31 Section 95A of the *Privacy Act* provides a similar mechanism to s 95. The current *Guidelines Approved under Section 95A of the Privacy Act 1988*[37] (Section 95A Guidelines) were issued in 2001.

Section 95 and 95A Guidelines

64.32 Both the Section 95[38] and 95A Guidelines[39] provide a detailed framework within which HRECs must consider the privacy implications of research proposals involving the use of individuals' personal or health information. HRECs may approve research proposals seeking to use identifiable personal or health information without consent only on the basis that the public interest in the research substantially outweighs the public interest in maintaining the level of privacy protection provided by the IPPs and the NPPs.

64.33 In considering this balance, HRECs are asked to consider a long list of matters including:

- the degree to which the personal information is necessary for the research;
- the public importance of the research and the likely contribution to the community;
- any likely benefits to individuals or groups;
- whether the research could be achieved within the terms of the IPPs and NPPs and the degree to which this would impact on the scientific value of the research;
- whether the risk of harm to the individual whose personal information is to be used is minimal;
- the study design and scientific credentials of those involved in the research;
- whether access to the information is restricted to appropriate personnel;
- the procedures to be followed to ensure that the information is permanently de-identified before the publication of results; and

---

37 National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

38 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000).

39 National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

- the procedures to be followed at the completion of the study to protect or destroy the information.[40]

64.34 The guidelines also address issues such as: preparing a proposal for approval by an HREC; and procedures to be followed in the collection, use or disclosure of personal or health information for research or the compilation or analysis of statistics.

64.35 The Section 95 and 95A Guidelines do not apply to the collection, use and disclosure of health information by agencies or organisations that are not covered by the *Privacy Act*. For example, the Act does not apply to state public sector entities, including public teaching hospitals and associated research bodies, where such bodies are established for a public purpose under a law of a state.[41] These organisations, however, may be covered by state legislation.[42]

---

40 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.3]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [D.5].

41 *Privacy Act 1988* (Cth) s 6C.

42 See, eg, *Health Records Act 2001* (Vic) HPPs 1.1(e)(iii), 2.2(g)(iii).

65. Research: Recommendations for Reform

Contents

Introduction

65.1 Chapter 64 sets out the special arrangements in place under the *Privacy Act 1988* (Cth) to allow for the use of personal information without consent in health and medical research. As discussed in that chapter, these arrangements are currently limited to the use of: personal information for medical research under the Information Privacy Principles (IPPs); and the use of health information for research, or the compilation or analysis of statistics, relevant to public health or public safety under the National Privacy Principles (NPPs).

65.2 This chapter considers whether these arrangements should be extended to include the use of personal information in other types of research in areas such as criminology and sociology. The chapter also considers the relationship between the research provisions of the *Privacy Act* and the *National Statement on Ethical Conduct in Human Research*[1] (the National Statement), as well as the role of Human Research Ethics Committees (HRECs) in considering the public interest balance.

1 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

Section 95 and 95A Guidelines

65.3 As discussed in Chapter 64, the *Guidelines under Section 95 of the Privacy Act 1988*[2] (the Section 95 Guidelines) relate to research conducted by public sector agencies bound by the IPPs. The *Guidelines approved under Section 95A of the Privacy Act 1988*[3] (the Section 95A Guidelines) relate to research conducted by private sector organisations bound by the NPPs. For a range of reasons, including differences in the enabling provisions, the two sets of guidelines are not identical. The Office of the Privacy Commissioner's (OPC) review of the private sector provisions of the *Privacy Act* (the OPC Review) noted stakeholder concerns that having two sets of guidelines gives rise to inconsistency and confusion, leading to conservative and incorrect decision making.[4] The National Health and Medical Research Council (NHMRC) expressed the view that this was hindering the conduct of effective health and medical research.[5]

65.4 A number of stakeholders, including the NHMRC, expressed strong support for a single set of principles and a single set of guidelines regulating health information in the conduct of health and medical research.[6] In response, the OPC Review stated that 'the *Privacy Act* is not intended to restrict important medical research'[7] and made the following recommendation:

> As part of a broader inquiry into the *Privacy Act* … the Australian Government should consider … how to achieve greater consistency in regulating research activities under the *Privacy Act*.[8]

Discussion Paper proposals

65.5 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72),[9] the ALRC proposed that the arrangements under the *Privacy Act* for conducting research should be streamlined, and noted that a nationally consistent privacy regime applying to both agencies and organisations, including a single set of Unified Privacy Principles (UPPs), would eliminate the problems inherent in maintaining two sets of research guidelines.

---

2 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000).

3 National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

4 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 201.

5 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

6 NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006; Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Australian Academy of Science, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 18 January 2005.

7 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 199.

8 Ibid, rec 62 (in part).

9 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007).

The ALRC proposed that the Privacy Commissioner issue a set of rules to replace the Section 95 and 95A Guidelines.[10]

65.6 The change from 'guidelines' to 'rules' was based on proposals made in Chapter 44 of DP 72. In that chapter, the ALRC examined the powers of the Privacy Commissioner to issue binding rules and advisory guidelines and expressed the view that the *Privacy Act* should distinguish between these types of instrument. The ALRC proposed that where 'guidelines' are legally binding they should be called 'rules'.[11] As stakeholders had not raised concerns about the fact that the Section 95 and 95A Guidelines were binding, the proposed research rules also were expressed to be binding.

65.7 The ALRC also put forward proposed research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle,[12] discussed further below. Although each principle requires an exception to allow the collection, use and disclosure of personal information for research purposes, one set of rules would apply to such collection, use and disclosure.

65.8 In DP 72, the ALRC also proposed that the research exceptions—currently limited to health and medical research—should be extended to cover all human research.[13] In these circumstances, it would no longer be appropriate for the NHMRC to develop and issue the research rules, as is currently the case, because of its focus on health and medical research. A wider range of agencies and organisations would need to be involved, and it was the ALRC's intention that the Privacy Commissioner would coordinate this consultation and development process.

65.9 The ALRC anticipated, however, that these rules would be developed by drawing upon the expertise of relevant stakeholders—most notably the NHMRC, the Australian Research Council and Universities Australia. The ALRC also proposed, therefore, that the Privacy Commissioner consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle. The ALRC noted that this consultation process would be an opportunity to ensure that the research rules and the National Statement were compatible.[14]

Submissions and consultations

65.10 Submissions and consultations to this Inquiry consistently made clear that having two different regimes regulating health and medical research under the IPPs and

10 Ibid, Proposal 58–1.
11 Ibid, Proposal 47–2.
12 Ibid, Proposals 58–8, 58–9.
13 Ibid, Proposal 58–2.
14 Ibid, Proposal 58–5.

the NPPs and, in particular, two sets of guidelines (the Section 95 and 95A Guidelines), creates confusion and adds significantly to the cost and complexity of seeking approval to conduct research. There was strong support in submissions and consultations for the development of a unified regime to regulate research, including a single set of guidelines.[15]

65.11 The CSIRO stated that:

> The current policy environment regarding privacy of personal information is complex and difficult to navigate. It is quite time-consuming to ensure that a given project will be compliant with all of the relevant legislation and codes of practice. This can add significantly to the set up costs of research projects, particularly where they involve health data. In addition, and most importantly, it also means that there is a delay of up to two years in initiating research projects, and a corresponding delay in the Australian people and society's acquisition of the benefits of the research outcomes.[16]

65.12 The Department of Health and Ageing (DOHA) submitted that:

> Recent reports on the operation of the *Privacy Act* and on research have both concluded that the present fragmentation and inconsistency in privacy regulation is proving to be a major impediment to health and medical research.
>
> The Department supports the development of a single set of guidelines regulating health information in the conduct of research, to support these activities at the institutional, multi-institutional and national levels. In keeping with the objective of achieving national consistency, there should also be alignment between the privacy principles covering research and the NHMRC's *National Statement on Ethical Conduct in Human Research* (National Statement).[17]

65.13 The OPC expressed support for a single set of rules to regulate research, but did not agree that these rules should be issued by the Privacy Commissioner. The OPC stated that the current arrangement, whereby the NHMRC issues guidelines, with approval from the Privacy Commissioner, worked well and did not require amendment.[18]

---

15 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Australian Institute of Criminology, *Submission PR 461*, 12 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Australian Commission on Safety and Quality in Health Care, *Submission PR 252*, 14 March 2007.

16 CSIRO, *Submission PR 176*, 6 February 2007.

17 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

18 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

65.14 A number of stakeholders expressed support for the proposal to develop rules in consultation with relevant stakeholders and to ensure that the rules and the National Statement were compatible.[19] The Public Interest Advocacy Centre (PIAC) suggested that consumer representatives should be involved in the development process.[20] The NHMRC noted that it would be pleased to assist the Privacy Commissioner in the development of the research rules.[21]

ALRC's view

65.15 The issues of complexity, fragmentation and inconsistency in the privacy regime generally, are discussed in detail in Part C of this Report. Chapter 4 includes a number of recommendations aimed at achieving greater national consistency. Part D recommends a single set of UPPs applying to agencies and organisations. A nationally consistent privacy regime applying both to agencies and organisations, and including a single set of UPPs, would eliminate the need for two sets of research guidelines.

65.16 The ALRC recommends, below,[22] that the 'Collection' principle and the 'Use and Disclosure' principle in the model UPPs include exceptions for the conduct of research using identified or identifiable personal information without consent. It is further recommended that any such research: be subject to HREC review; and be conducted in accordance with binding rules issued by the Privacy Commissioner. There should be one set of rules issued under the model UPPs covering the collection, use and disclosure of identified or reasonably identifiable personal information in the conduct of research, and these 'Research Rules' should replace the Section 95 and 95A Guidelines.

65.17 While the Section 95 and 95A Guidelines are issued by the NHMRC and approved by the Privacy Commissioner, the new Research Rules should be issued by the Privacy Commissioner. This approach is recommended for three reasons. First, the research exceptions allow the use of personal information in ways that, under normal circumstances, would be a breach of the UPPs. In this respect the research exceptions, and the rules issued under those exceptions, are similar in effect to Public Interest Determinations (PIDs). As discussed in detail in Chapter 47, PIDs are developed and 'made' by the Privacy Commissioner. This level of involvement and control by the regulator is appropriate in circumstances where the level of protection provided by the UPPs is to be modified.

---

19 Confidential, *Submission PR 570*, 13 February 2008; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

20 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

21 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

22 Recs 65–8, 65–9.

65.18 By way of contrast, privacy codes, developed by industry and 'approved' by the Privacy Commissioner, cannot derogate from the protection provided by the UPPs. This distinction is important. Where collection, use and disclosure of personal information are to be allowed in circumstances that derogate from the UPPs, the Privacy Commissioner should retain primary responsibility for the development and issuance of the rules that regulate that activity.

65.19 Secondly, the ALRC recommends, below, that the research exceptions currently applying to health and medical research should be extended to cover all human research.[23] In these circumstances, it would no longer be appropriate for the NHMRC alone to develop and issue the Research Rules. A wider range of agencies and organisations will need to be involved in developing the rules and the Privacy Commissioner is well placed to play a coordinating role. As mentioned above, the ALRC anticipates that the rules will be developed in consultation with, and drawing on the expertise of, key stakeholders.

65.20 Thirdly, the ALRC recommends in Chapter 3 that the Australian Government and state and territory governments establish a Commonwealth-state cooperative scheme in relation to the handling of personal information. Under the recommended scheme, the states and territories would enact legislation to regulate the handling of personal information in that state or territory's public sector, with all jurisdictions adopting the relevant UPPs and other elements of the *Privacy Act* into their legislation. This will include the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle, including the requirement for research to be conducted in accordance with Research Rules issued by the Privacy Commissioner. The Office of the Victorian Privacy Commissioner (OVPC) submitted that, if such rules are to apply to personal information held by state and territory public sector agencies, they will need to be developed in consultation with state and territory privacy commissioners and other relevant state and territory stakeholders.[24] The ALRC agrees.

65.21 In DP 72, the ALRC proposed that the Privacy Commissioner consult with relevant stakeholders to ensure that the approach adopted in the Research Rules and the National Statement are compatible. It is important to ensure that the Research Rules and the elements of the National Statement dealing with privacy are aligned to minimise confusion for research institutions, researchers and HRECs.

---

23 Rec 65–2.

24 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

Recommendation 65–1 (a) The Privacy Commissioner should issue one set of rules under the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle to replace the *Guidelines under Section 95 of the Privacy Act 1988* and the *Guidelines Approved under Section 95A of the Privacy Act 1988*.

(b) The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the 'Collection' and 'Use and Disclosure' principles—that is, the 'Research Rules'.

(c) Those elements of the *National Statement on Ethical Conduct in Human Research* dealing with privacy should be aligned with the *Privacy Act* and the Research Rules to minimise confusion for institutions, researchers and Human Research Ethics Committees.

Research in areas other than health and medical

65.22 NPP 10.3 currently provides an exception for the collection of health information without consent where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety. NPP 2.1(d) provides an exception for the use or disclosure of health information without consent where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety. Section 95 of the *Privacy Act* provides an exception from the IPPs for acts done by agencies 'in the course of medical research'.

65.23 Despite the differences between the exceptions in the NPPs and the exception in relation to the IPPs, the general intention clearly is to limit the exceptions to the field of health and medical research. The OPC Review recommended that the Australian Government consider whether there was a need to permit the use and disclosure of personal information for research that does not involve health information.[25]

65.24 The Council of Europe Committee of Ministers has recognised that the public interest in a range of research areas—including, but not restricted to, health and medical research—may outweigh the public interest in maintaining privacy protections.

> Any exception to that rule [that where sensitive personal information is collected for statistical purposes, it should be collected in non-identifiable form] can only be justified by major public interest, as where statistical information is needed to contain epidemics, combat the evil of drug taking, investigate the scale and pattern of sexual

25 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 60.

> assaults on minors or develop aid to social groups in difficulty. Such examples, to which many more might be added, relate to matters which affect society's essential interests and in which the state has responsibilities. In such cases the guarantees on protection of sensitive data must be adapted to the objective information needs arising from the public interest.[26]

65.25 Canadian privacy legislation allows private sector organisations to use or disclose personal information without consent where it is for 'statistical, or scholarly study or research'.[27] Canadian privacy legislation also allows public sector agencies to disclose personal information to any person or body for 'research or statistical purposes' in specified circumstances.[28]

65.26 The *Data Protection Act 1998* (UK) also allows data to be processed for 'research purposes'—which includes statistical or historical purposes—so long as the data are *not* processed: to support measures or decisions with respect to particular individuals; or in such a way as to cause, or be likely to cause, substantial damage or substantial distress to the data subject. The results of the research are not to be made available in a way that would identify the data subjects.[29]

65.27 The *Privacy Act 1993* (NZ) allows the use and disclosure of personal information for 'statistical or research purposes', so long as it is not published in a form that could reasonably be expected to identify the individuals concerned.[30]

65.28 The *Information Privacy Act 2000* (Vic) allows state agencies to use and disclose personal information where necessary for 'research, or the compilation or analysis of statistics, in the public interest'.[31] The *Personal Information Protection Act 2004* (Tas) has a similar provision.[32]

65.29 The ALRC asked a number of questions in the Issues Paper, *Review of Privacy* (IP 31),[33] about expanding the existing research exceptions in the *Privacy Act* to include other types of personal information or other fields of research. In DP 72, the ALRC proposed that the *Privacy Act* should be amended to extend the existing arrangements relating to health and medical research to cover human research more generally.[34]

---

26 Council of Europe—Committee of Ministers, *Explanatory Memorandum to Recommendation No R(97)18 of the Committee of Ministers to Member States Concerning the Protection of Personal Data Collected and Processed for Statistical Purposes* (1997), [85(b)].

27 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) ss 7(2)(c); 7(3)(f).

28 *Privacy Act* RS 1985, c P-21 (Canada) s 8(j).

29 *Data Protection Act 1998* (UK) s 33.

30 *Privacy Act 1993* (NZ) s 6.

31 *Information Privacy Act 2000* (Vic) sch 1, IPP 2(c).

32 *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(c).

33 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–13, 4–32, 8–26.

34 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–2.

Submissions and consultations

65.30 The OPC expressed support for allowing the collection, use and disclosure of personal information—rather than just health information—for health and medical research, and for research relevant to public health or public safety. This was on the basis that such research may be advanced by the linking of health information with other forms of personal information. However, the OPC did not support expanding the existing arrangements to cover human research more generally.[35]

65.31 The OPC submitted that the public interest in health-related research was likely to be greater than the public interest in other social research. The OPC was also concerned that the proposed extension would lead to the use of personal information for research 'in areas that may be unforeseen, unexpected and potentially undesirable'.[36] The Australian Privacy Foundation would support the proposed extension only on the basis that the public interest test, discussed below, was maintained in its current form.[37]

65.32 Where the public interest in a particular research proposal outside the health and medical field was likely to outweigh the public interest in maintaining the level of protection provided by the privacy principles, the OPC suggested that a PID should be sought in relation to the proposal.[38] To date, two such PIDs have been granted by the Privacy Commissioner:

- PID 5—Disclosure of personal information contained in homicide files in the ACT to the Australian Institute of Criminology (AIC) for research purposes;[39] and

- PID 8—Disclosure of personal information contained in certain Commonwealth Director of Public Prosecution files that relate to serious incidences of fraud, dishonesty and deception to the AIC for research purposes.[40]

65.33 The AIC submitted that a great deal of criminological research requires access to personal information collected by police, courts, correctional agencies, regulatory bodies and health service providers in the course of their duties. Because consent to use and disclose this information for research purposes is not built into the collection of the information, it is difficult to conduct research using the information within the existing provisions of the *Privacy Act*. The AIC highlighted the delay and resources involved in applying for a PID, and expressed support for extending the regime in the *Privacy Act*

---

35 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
36 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
37 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
38 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
39 Privacy Commissioner, *Public Interest Determination 5*, effective 14 December 1991.
40 Privacy Commissioner, *Public Interest Determination 8*, effective 26 August 2002.

to allow such research to proceed without the need to seek a PID.[41] On the issue of public interest, the AIC stated:

> Criminological research does have a profound impact on individuals and the community … Research into practices and programs can … reduce the likelihood of re-offending with consequent reductions in the number of victims of crime ... Much of the research undertaken by the AIC is of this nature and has the potential through its contribution to evidence-led policy, to reduce crime and crime-related harms resulting in significant positive outcomes for the community.[42]

65.34 Other agencies and organisations also expressed support for expanding the research exceptions to cover research other than health and medical research. National Legal Aid noted that it holds significant amounts of personal information that is in demand for social and legal research. It stated that:

> We believe that ethically informed and regulated research has an essential role to play in addressing issues of disadvantage, and promoting informed policy on criminal law enforcement. However it is important to reconcile the sometimes competing priorities of researchers and research subjects in a way that does not sacrifice one to the other or undermine the autonomy and dignity of the most disadvantaged groups.[43]

65.35 The Australian Bureau of Statistics (ABS) noted that:

> More generally, through its work on health and social statistics, the ABS is aware that the community expects its information to be used effectively both at the point of service provision for the individual, and also in research for the public good. In balancing privacy against public benefit of research, there is a need to recognise this broad, but not necessarily vocal, community support for using information to achieve better social outcomes.[44]

65.36 The CSIRO noted that it can be difficult to draw a clear line between 'health' and 'non-health' information and 'health' and 'social sciences' research. It stated that researchers are increasingly seeking to integrate health and non-health personal information in order to answer complex research questions. For example, it noted that health and educational experiences—in combination rather than separately—are fundamental to outcomes for children and youth.

> We believe that extending the federal privacy principles to allow agencies and organisations to collect non-health related sensitive information for purposes including research and statistics is highly desirable. This is because researchers are seeking to address increasingly complex questions involving health and lifestyle information, for example to determine how environmental factors influence genetic predisposition to disease.[45]

---

41 Australian Institute of Criminology, *Submission PR 461,* 12 December 2007. For example, the application for PID 8 was lodged on 7 January 2002, signed by the Privacy Commissioner on 22 March 2002 and tabled in Parliament on 26 August 2002.

42 Ibid.

43 National Legal Aid, *Submission PR 521,* 21 December 2007.

44 Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

45 CSIRO, *Submission PR 176,* 6 February 2007.

65.37 The Western Australian Department of Health agreed about the difficulties involved in distinguishing health and medical research from other research, and noted that social indicators are increasingly being used to understand health outcomes.[46] The Australian Federal Police (AFP) noted the importance of research in the criminal justice field, and pointed to PID 5 as an example of this.[47]

65.38 The Government of South Australia expressed support for expanding the arrangements to include social science research, as well as criminological research.

> Social science research on key social issues is of critical importance to the community. There is a growing recognition of the importance of evidence-based practice in the social services and the use of research and evaluation in improving policy and service planning. Robust research, based on quality data, is required to provide the necessary evidence and directions for dealing with significant social issues, such as child abuse, family violence or homelessness. Data held by government and NGOs can contribute to better understanding of such issues and the development of effective solutions. Whilst obtaining individuals' consent would be desirable it is often not possible, particularly from those clients who are highly transient and harder to engage, are in a non-voluntary relationship (for example, child protection) or in the case of large-scale studies (such as population-based data matching).[48]

65.39 There was strong support among other key stakeholders—including the NHMRC, the Australian Research Council, DOHA, the Commonwealth Ombudsman and a number of Australian Universities—for expanding the *Privacy Act* arrangements to include other fields of research so long as safeguards, similar to those currently in place in relation to health and medical research, were applied.[49] While expressing

---

46 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

47 Australian Federal Police, *Submission PR 186*, 9 February 2007.

48 Government of South Australia, *Submission PR 187*, 12 February 2007.

49 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; CSIRO, *Submission PR 176*, 6 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Confidential, *Submission PR 143*, 24 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Insolvency and Trustee Service Australia, *Submission PR 123*, 15 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Australian Research Council, *Consultation PC 181*, Canberra, 22 October 2007.

support for expanding the arrangements to include human research more generally, a few noted the additional burden this was likely to place on HRECs.[50]

ALRC's view

65.40 There is no in-principle reason to limit the arrangements for research under the *Privacy Act* to health and medical research. The ALRC notes that the research exceptions in other jurisdictions, such as the United Kingdom, Canada and New Zealand, are expressed in broad terms. Other areas of research, such as sociology and criminology, have a strong public interest basis because of their potential to lead to evidence-based policy development and significant positive outcomes for the community. The *Privacy Act* should not be impede such research. Further, the ALRC recognises that research increasingly involves multi-disciplinary approaches, that non-health information is often crucial to health and medical research and that, in any event, it is sometimes difficult to define what amounts to health and medical research and what does not.

65.41 The ALRC notes that the National Statement and its oversight mechanisms, such as review by HRECs, apply to all human research—that is, research 'conducted with or about people, or their data or tissue'. The existing regime in relation to health and medical research under the *Privacy Act* relies to a certain extent on the safeguards provided by the National Statement and, in particular, on review of research proposals by HRECs. Those safeguards can be applied to research more generally. The ALRC recommends below that any research that proposes to use personal information in a way that is inconsistent with the model UPPs should be subject to HREC review.[51] In order for such research to proceed, an HREC will have to be satisfied that the public interest in the research outweighs the public interest in maintaining the level of privacy protection provided by the UPPs.

65.42 In addition, the *Privacy Act* can, and should, include a range of limits and safeguards, discussed below, to ensure that personal information is used without consent for research purposes only in appropriate circumstances, for example:

- where the research cannot be undertaken using personal information that does not identify individuals;
- it is unreasonable or impracticable to seek individuals' consent to the collection, use or disclosure of their information; and
- the research is conducted in accordance with rules issued by the Privacy Commissioner.

---

50 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

51 Recs 65–8, 65–9.

65.43 The ALRC recommends, therefore, that the *Privacy Act* be amended to extend the arrangements relating to the collection, use and disclosure of personal or health information in health and medical research to include the collection, use and disclosure of personal information in human research more generally.

Recommendation 65–2 The *Privacy Act* should be amended to extend the arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

Definition of research

65.44 Given the proposed expansion of the arrangements relating to research under the *Privacy Act*, the ALRC has considered whether it is necessary to define the term 'research' for the purposes the Act. Section 6 of the *Privacy Act* currently states that 'medical research includes epidemiological research', but the term is not otherwise defined.

65.45 The IPPs do not refer to health or medical research, but s 95 of the *Privacy Act*—which establishes the research exception to the IPPs and provides for the development of the Section 95 Guidelines—refers to 'medical research'.[52] The NPPs refer to research, or the compilation or analysis of statistics, relevant to public health or public safety. The NHMRC has expressed the view that there is no obvious rationale for the differences between the approach to research taken by s 95 of the *Privacy Act* and the NPPs.[53]

65.46 The National Statement makes the point that:

> There is no generally agreed definition of research; however, it is widely understood to include at least investigation undertaken to gain knowledge and understanding or to train researchers.[54]

65.47 Rather than attempting to define 'research', the National Statement adopts a contextual approach. It attempts to define those activities that should fall under the National Statement, by asking the following two questions:

---

52 Section 73 of the *Privacy Act*, which deals with applications for PIDs by the NHMRC, also refers to 'medical research'.

53 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

54 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), 7.

- What is human research?

- When and by what means does human research, or other activities such as quality assurance or improvement, or clinical audit, need ethical review?

65.48 As noted above, human research is defined broadly in the National Statement as research 'conducted with or about people, or their data or tissue'. The National Statement then sets out the circumstances in which such research requires ethical review:

> Research with more than a low level of risk … must be reviewed by an HREC. Research involving no more than low risk may be reviewed under other processes ... Institutions may also determine that some human research is exempt from ethical review.[55]

65.49 Risk is defined as potential for harm, discomfort or inconvenience and involves:

- the likelihood that a harm (or discomfort or inconvenience) will occur; and

- the severity of the harm, including its consequences.[56]

65.50 In DP 72, the ALRC suggested that the term 'research' in the *Privacy Act* should be defined only by reference to the National Statement. The existing regime in relation to health and medical research under the *Privacy Act* and the Section 95 and 95A Guidelines relies on structures established in the National Statement and, in particular, on review of research proposals by HRECs. The new research regime proposed in DP 72, and recommended in this Report, continues to rely on these safeguards. For this reason the ALRC proposed that 'research', for the purposes of the *Privacy Act*, should be limited to those activities subject to review by an HREC under the National Statement.[57]

65.51 The ALRC also proposed that the definition of research expressly include 'the compilation and analysis of statistics'.[58] While it is possible to argue that the term 'research' is broad enough to include the compilation or analysis of statistics, this is not universally accepted. The proposal was intended to put the matter beyond doubt for the purposes of the *Privacy Act*.

---

55 Ibid, 8.
56 Ibid, 15.
57 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–3.
58 Ibid, Proposal 58–3.

Submissions and consultations

65.52 DOHA noted in relation to the draft *National Health Privacy Code*[59] that:

> In relation to the definition of the term 'research' … the approach taken in NHPP 1 of the draft Code was to leave the term undefined, but to refer to the activities of 'research or the compilation or analysis of statistics'. There is room within the guidelines designed to support the application of this principle, to provide guidance on the meaning of the term 'research'. Such an approach would appear to be appropriate and effective.[60]

65.53 A number of other stakeholders, however, were of the view that it was important to include a definition of the term 'research' in the *Privacy Act*.[61] Others expressed support for the approach adopted in the National Statement.[62] The Office of the Health Services Commissioner in Victoria expressed the view that any definition should be consistent with the National Statement, as the recent review and redrafting of that document had been a very thorough process.[63]

65.54 The AIC expressed strong support for the ALRC's proposal to define research as those activities subject to review by an HREC under the National Statement, noting that this approach would ensure consistency between the *Privacy Act* and the National Statement. The AIC was of the view that this alignment would assist researchers and HRECs in their decision making.[64] Other stakeholders supported this proposal;[65] for example, the University of Newcastle submitted that 'the compilation and analysis of statistics' should be clearly included;[66] and the Western Australian Department of Health stated that the principle purpose of defining the term 'research' in the *Privacy Act* would be to distinguish those activities that must be given independent review by an HREC.[67]

---

59 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003).

60 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

61 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Council of Social Service of New South Wales, *Submission PR 115*, 15 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

62 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006.

63 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

64 Australian Institute of Criminology, *Submission PR 461*, 12 December 2007.

65 Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

66 University of Newcastle, *Submission PR 413*, 7 December 2007.

67 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

65.55 On the other hand, the OPC argued that the *Privacy Act* should not attempt to define the term 'research' by reference to the National Statement. The OPC was concerned that the National Statement was not legally binding and might change over time. The OPC also suggested that the link between the research exceptions in the *Privacy Act* and review by HRECs could be achieved more directly by making such review a requirement in the research exceptions.[68]

65.56 Professor Colin Thomson, of the University of Wollongong, also expressed the view that any attempt to link the definition of research in the *Privacy Act* to the National Statement would cause confusion. He noted that the National Statement included three definitions: 'research'; 'human research'; and 'human research subject to ethical review'. To define the term 'research' in the *Privacy Act* as any activity subject to review by an HREC under the National Statement would involve conflating these terms in a potentially confusing way.[69]

ALRC's view

65.57 The ALRC notes that there is no generally agreed definition of research, and acknowledges the concerns raised by stakeholders in relation to linking a definition of research in the *Privacy Act* with the National Statement. Following further consideration, the ALRC concludes that it is unnecessary to make this link by defining the term 'research' in the *Privacy Act* by reference to the National Statement. The ALRC agrees with the OPC that the crucial link can be made simply by requiring that research proposing to collect, use or disclose personal information in breach of the model UPPs must be reviewed by an HREC that is constituted in accordance, and acting in compliance, with the National Statement as in force from time to time. This requirement is included expressly in the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle recommended below.[70]

65.58 While it is possible to argue that the term 'research' is broad enough to include the compilation or analysis of statistics, this is not universally accepted. The NPPs refer to research, *or* the compilation or analysis of statistics. This wording tends to infer that research does not include the compilation or analysis of statistics. The National Statement does not refer to the compilation or analysis of statistics, but HRECs are asked to review research proposals consisting of the compilation or analysis of statistics or including statistical elements. In order to put the matter beyond doubt, the ALRC recommends that the *Privacy Act* should state expressly that the term 'research' includes 'the compilation and analysis of statistics'.

---

68 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
69 C Thomson, *Submission PR 454*, 7 December 2007.
70 Recs 65–8, 65–9.

Recommendation 65–3 The *Privacy Act* should be amended to provide that 'research' includes the compilation or analysis of statistics.

The public interest balance

65.59 In the second reading speech for the Privacy Amendment (Private Sector) Bill 2000 (Cth), the then Attorney-General, the Hon Daryl Williams AM QC MP, stated that:

> The balance between the interests of privacy and the need to facilitate medical research was an issue that the Privacy Commissioner and the government looked at closely. The bill provides that, where information is collected for research purposes, it must be collected with consent or, where this is not practicable, in accordance with strict safeguards set out in the bill. In addition, researchers must take reasonable steps to de-identify personal information before the results of research can be disclosed.[71]

65.60 The *Privacy Act* requires the Privacy Commissioner to be satisfied before approving guidelines under ss 95 or 95A, that the public interest in the relevant research outweighs to a substantial degree the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs.

65.61 The Section 95 and 95A Guidelines include a similar public interest test. Where research may breach the IPPs or NPPs, the Guidelines provide that the research must be approved by an HREC. Before approving a particular research proposal under the Guidelines, HRECs are required to consider whether the public interest in the research *substantially* outweighs the public interest in the protection of privacy.[72] In considering the public interest balance, HRECs are required to consider certain specified matters including:

- the value and public importance of the research;
- the likely benefits to the participants;
- whether the research design can be modified;
- the financial costs of not proceeding with the research;

---

71 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).

72 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), Guideline 3.2; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), Guideline D.4.

- the type of personal information being sought;
- the risk of harm to individuals; and
- the extent of a possible breach of privacy.

65.62 A number of stakeholders making submissions to the OPC Review argued that the *Privacy Act* and the Section 95 and 95A Guidelines fail to achieve an appropriate public interest balance. In his submission—the text of an address to the Australian Epidemiological Association—Dr Richie Gun of the Department of Public Health, University of Adelaide, discussed the particular difficulties faced by epidemiologists, and the problems he has faced in gaining access to data in cancer registries.

> In Australia we are now in a uniquely advantageous position to carry out such research, as we have mandatory registration of cancers in every State and Territory. We therefore have almost complete enumeration of all invasive cancers occurring in Australia, with the potential to carry out epidemiological studies on cancer incidence equal to or better than anywhere else in the world. Unfortunately privacy laws are impeding access to cancer registry data, so that it is becoming increasingly hard to carry out the linkage of cancer registrations with exposure data.[73]

65.63 The OPC Review stated that:

> There is considerable evidence that key researchers, especially epidemiological researchers, consider that the current balance between privacy and the public benefit of research is too heavily weighted in favour of individual privacy to the detriment of research. By gaining access to population data and data linkage, the research might considerably benefit disadvantaged groups that are currently under researched.[74]

65.64 The OPC Review went on to recommend that:

> As part of a broader inquiry into the *Privacy Act* … the Australian Government should consider … where the balance lies between the public interest in comprehensive research that provides overall benefits to the community, and the public interest in protecting individuals' privacy (including individuals having choices about the use of their information for such research purposes).[75]

65.65 In DP 72, the ALRC considered two situations in which the public interest currently must be weighed in relation to research—that is, where the Privacy Commissioner is approving research guidelines, and where HRECs are approving research proposals. The ALRC proposed that the Privacy Commissioner take primary responsibility for developing and issuing the Research Rules under the research exceptions to the UPPs.[76] The ALRC did not consider it necessary that the Privacy

---

73 University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

74 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

75 Ibid, rec 60.

76 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–1.

Commissioner should be required expressly to consider the public interest in developing these rules. In exercising his or her powers under the *Privacy Act*, the Commissioner is currently required to have regard to the matters set out in s 29, which include the balance of public and private interests.

65.66 In this Report, the ALRC recommends that the *Privacy Act* be amended to require the Commissioner, in exercising his or her powers, to have regard to the matters set out in the objects clause.[77] That clause, discussed in Chapter 5, expressly recognises that the right to privacy is not absolute and that the *Privacy Act* provides a framework within which to balance the public interest in protecting the privacy of individuals with other public interests. The Privacy Commissioner would be required to take these matters into account when developing the Research Rules.

65.67 In DP 72, the ALRC also proposed that, where an HREC was of the view that the public interest in a particular research proposal going forward *outweighed* the public interest in maintaining the level of privacy protection provided by the model UPPs, the research should be allowed to proceed. The ALRC noted that the public interest in protecting the right to privacy must be considered in the context of other rights and other public interests. The ALRC suggested that it is not the degree to which one public interest outweighs another—whether slightly or substantially—that should be at issue. Rather, the ALRC proposed that the test to be applied by HRECs should be whether the public interest in a particular research activity 'outweighs'—rather than 'substantially outweighs'—the public interest in maintaining the level of privacy protection provided by the UPPs.[78]

Submissions and consultations

65.68 The OPC submitted that the current public interest test was appropriate—that is, where research proposes to use identifiable personal information without consent, the public interest in the research must 'substantially outweigh' the public interest in the protection of privacy.[79] The OPC noted that, in general,

> individuals expect to be given the opportunity to consent to the handling of their health information for research purposes. The section 95 and 95A mechanisms provide a way of ensuring that important health and medical research can be undertaken in circumstances where the community's expectations around consent cannot be met. The mechanisms provide a sound framework of accountability and oversight of the handling of health information without consent.[80]

---

77 Rec 46–3.

78 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–4.

79 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

80 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

65.69 The OPC also noted that

> privacy safeguards are necessary for research to remain effective. If individuals do not feel that their personal information is going to be appropriately protected, they may avoid treatment, or may supply partial or inaccurate information to the detriment of their clinical well-being and the ultimate quality of any research which may utilise their health information.[81]

65.70 DOHA submitted that:

> The Department considers that the appropriate test for an HREC, considering a research proposal, is that the Committee must be satisfied that the public interest in the proposed activity 'substantially outweighs' the public interest in the protection of privacy ... Health information collected in the delivery of healthcare services is subject to a legal duty of confidence. In order to comply with this duty, express consent would normally be required before health information was disclosed for research purposes. It would not appear sufficient to discharge this duty by 'finely' balancing the public interests. The balance should be 'clearly' in favour of the research.[82]

65.71 A number of other stakeholders also expressed support for maintaining the current public interest test.[83] Professor Thomson expressed the view that the 'substantially outweighs' test requires an unequivocal choice to be made and that this may add clarity to the decision-making process for HRECs.[84]

65.72 On the other hand, there was significant support for modifying the test to allow research to proceed where the public interest in the research outweighs the public interest in maintaining the level of privacy protection provided by the UPPs.[85] Support came from a diverse range of stakeholders including the Government of South Australia, PIAC, Medicare Australia, Privacy NSW, the AIC, the University of Western Sydney HREC, the NHMRC and the Australian Research Council.

---

81 Ibid.

82 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

83 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

84 C Thomson, *Submission PR 454*, 7 December 2007.

85 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Australasian Epidemiological Association, *Submission PR 473*, 14 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australian Institute of Criminology, *Submission PR 461*, 12 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Australian Research Council, *Consultation PC 181*, Canberra, 22 October 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006.

65.73 The Office of the Health Services Commissioner in Victoria stated that the 'current definition with the use of the words "substantially outweighs" has lead to ethics committees taking an overly conservative approach', and suggested that the approach adopted in the draft *National Health Privacy Code* would be more appropriate.[86] NHPP 1 of the draft Code provides that research must be in the public interest in order for it to proceed, but that it must proceed in accordance with rules issued for the purpose.

65.74 The NHMRC was very clearly of the view that

> the current requirement in the *Privacy Act* and the Section 95 and Section 95A Guidelines that the public interest in research 'substantially outweighs' or 'outweighs to a substantial degree' the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs is unbalanced and is limiting the conduct of important health and medical research …
>
> In undertaking an assessment for the purposes of determining the balance of public interests, an HREC routinely assesses a range of issues, which are detailed in [IP 31]. This assessment provides a robust framework and in our view protects the reasonable interests of individuals. It is clear that an assessment would not favour research that has the potential to cause significant harm to individuals.
>
> We consider that a more appropriate and effective test that would accord with community sentiment would simply be that the balance of public interests favours the research proceeding.[87]

65.75 The Alfred Hospital Ethics Committee commented that any changes to the privacy rules governing research should aim to clarify and refine the public interest test. The Committee was generally supportive of the ALRC's proposed approach in this area, including the removal of the term 'substantially' from the public interest test. The Committee found the term confusing and believed it led to inconsistent decision making.[88]

65.76 Professor Thomson noted that there was evidence that HRECs were not unduly constrained by the 'substantially outweighs' test. He quoted a 2004 NHMRC report which indicated that, of 60 medical research proposals considered under the Section 95 Guidelines, 58 were approved, and of 70 proposals considered under the Section 95A Guidelines, 64 were approved.[89]

---

86 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

87 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

88 General Ethical Issues Sub-Committee—Alfred Hospital Ethics Committee, *Submission PR 531*, 21 December 2007.

89 C Thomson, *Submission PR 454*, 7 December 2007; National Health and Medical Research Council, *Report of the 2002–03 HREC Annual Report Process* (2004).

65.77 The OPC suggested that, even if the current provisions were leading to overly conservative decision making by HRECs, an appropriate response would be greater education and training of HRECs. In addition, the OPC considered that

> harmonising the existing provisions would also likely assist in simplifying HRECs decision making. Reducing any uncertainty about legal requirements may give HRECs greater confidence in applying the legal test. Conversely, a lack of certainty may promote a risk averse and conservative approach to decision making.[90]

ALRC's view

65.78 The ALRC agrees with the OPC that harmonising elements of the current regime regulating the use of personal information in the research context should assist HRECs' decision making. These issues are addressed by other recommendations in this Report, including the recommendations in Chapter 3, aimed at national consistency, and Recommendation 18–2 on the establishment of a single set of UPPs.

65.79 In considering the public interest test itself, it is important to keep in mind the other limits and safeguards that apply to research using personal information without consent under the *Privacy Act*. The existing provisions of the Act allow such research to proceed only on the basis that the research cannot be undertaken with information that does not identify individuals; it is impracticable to seek consent from those individuals; and the research is conducted in accordance with the Section 95 or 95A Guidelines. The recommendations in this Report would allow such research to proceed only where the research cannot be undertaken with information that does not identify the individual; it is unreasonable or impracticable for the agency or organisation to seek the individual's consent; and the information is collected, used and disclosed in accordance with rules issued by the Privacy Commissioner.

65.80 The Section 95 and 95A Guidelines also require HRECs to consider: whether access to the information is restricted to appropriate personnel involved in the research; the procedures in place to ensure that personal information is permanently de-identified before the publication of results; and the procedures in place to ensure the security of the information and when it will be destroyed or returned to the original data custodian.[91] The ALRC anticipates that similar safeguards will be included in the Research Rules to be issued by the Privacy Commissioner.

65.81 The ALRC has carefully considered the divergent views on this important issue expressed in submissions and consultations. Chapter 1 examines the right to privacy in some detail and notes that the right is not absolute. The public interest in protecting this private right must be considered in the context of other rights and other public interests. In the ALRC's view, it is not the degree to which one public interest

---

90 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

91 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), 3.3; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), D.5.

outweighs another—whether slightly or substantially—that should be at issue. If, taking all relevant factors into account, the public interest in one course of action outweighs the public interest in another course of action, the appropriate course of action is clear. In particular—in the research environment where a range of other safeguards are in place—if the public interest in a particular research proposal going forward outweighs the public interest in maintaining the level of privacy protection provided by the privacy principles, then the research should be allowed to proceed.

65.82 The ALRC has recommended above that the areas of research and the kinds of personal information available to researchers should be broadened. The public interest test should be the same for all human research.

65.83 Recommendations 65–8 and 65–9, below, set out research exceptions to the 'Collection' and 'Use and Disclosure' principles. These exceptions require an HREC to review research that proposes to collect sensitive information without consent, or to use or disclose personal information without consent, and be satisfied that the public interest in the research activity outweighs the public interest in maintaining the level of privacy protection provided by *Privacy Act*. The Section 95 and 95A Guidelines include guidance for HRECs in considering the balance of public interests. It would be appropriate for the National Statement to include guidance for HRECs on this matter. The content of the rules to be issued by the Privacy Commissioner under the research exceptions, although not directed at HRECs, will also be of assistance.

Recommendation 65–4 The research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle should provide that, before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*.

Impracticable to seek consent

65.84 NPP 10 and NPP 2 allow the collection, use and disclosure of health information for research without consent where it is *impracticable* for the organisation to seek the individual's consent before the collection, use or disclosure. The Macquarie Dictionary defines 'impracticable' as 'not practicable; that cannot be put into practice with the available means'.[92] The National Statement provides that 'impracticable' may include

92 *Macquarie Dictionary* (online ed, 2007).

situations where the quantity, age or accessibility of the records makes it impracticable to obtain consent.[93]

65.85 The Section 95 Guidelines allow the collection, use or disclosure of personal information by agencies without consent when it is reasonable for the research to proceed without this consent.[94]

65.86 In its submission to the OPC Review, the NHMRC argued that the *Privacy Act* regime should allow the use and disclosure of health information in health and medical research where seeking consent may prejudice the scientific value of the research, or where the procedures necessary to obtain consent are likely to affect seriously and adversely the well being, including the psychological health, of the individual.[95] A number of other submissions to the OPC Review stated that the circumstances in which the NPPs allow the collection, use and disclosure of health information without consent are too narrow.[96]

65.87 In DP 72, the ALRC did not propose a change to the requirement that it be impracticable to seek the consent of individuals before collecting, using or disclosing their personal information for research purposes. This was on the basis that, although there is room for interpretation in regard to what amounts to 'impracticable' to seek consent, it appeared to be an appropriate element of the framework permitting the collection, use or disclosure of personal information without consent for research.

65.88 The ALRC did propose, however, that the Privacy Commissioner consult with relevant stakeholders in developing the rules to be issued under the research exceptions to ensure that the approach adopted in the rules and the National Statement were compatible.[97] The ALRC anticipated that the Privacy Commissioner would include in those rules guidance on the meaning of 'impracticable to seek consent'.

Submissions and consultations

65.89 In its submission, the OPC expressed the view that the framework contained in the NPPs for the use of health information in research without consent, including the requirement that it be 'impracticable to seek consent', is appropriate and effective and

---

93 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [2.3.6(c)].

94 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.2(a)].

95 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

96 Australian Compliance Institute Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004; University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004; Australasian Epidemiology Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004.

97 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–5.

did not support amendments to the framework. The OPC noted that whether it is impracticable to seek consent depends on the particular circumstances of the case, and that the OPC has issued guidance on the matter.[98] The OPC considered that organisations are required to take reasonable steps to seek consent and that there must be compelling justification to support the collection, use or disclosure of health information without consent. In the OPC's view, this means concrete and substantial obstacles, as opposed to mere inconvenience.[99]

65.90 The OPC provided the following examples of situations that might give rise to 'impracticality' for the purposes of the *Privacy Act*:

- individuals may be uncontactable due to death or relocation (this particularly arises in relation to old records);
- individuals may be part of a demographic group that is difficult to contact (for example, remote/indigenous groups);
- the number of records involved may cause logistical problems; or
- the objective of the investigation may need to be concealed from subjects in order to minimise various forms of bias (for example, having to obtain consent in blind trials could compromise the integrity of the research).[100]

65.91 The Australian Privacy Foundation also expressed support for the existing framework providing for the use of personal information in research where obtaining consent is impracticable.[101] The Australian Nursing Federation stated that the framework was appropriate, but that further guidance was needed as to the meaning of 'impracticable'.[102] A number of stakeholders expressed support for the proposition that the *Privacy Act* and the National Statement should be consistent.[103]

65.92 On the other hand, some stakeholders raised concerns about the use of the term 'impracticable'. The Alfred Hospital Ethics Committee stated that researchers and HRECs find the term confusing and suggested that 'unduly burdensome' or 'unreasonably onerous' would be clearer. The Committee noted that guidance was

---

98 Office of the Federal Privacy Commissioner, *Handling Health Information for Research and Management*, Information Sheet 9 (2001).

99 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

100 Ibid.

101 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

102 Australian Nursing Federation, *Submission PR 205*, 22 February 2007.

103 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australasian Epidemiological Association, *Submission PR 473*, 14 December 2007; Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

necessary on when the cost of obtaining consent would make it 'impracticable'.[104] The NHMRC, in particular, expressed concern, stating that:

> It is not clear to us whether it would be considered impracticable to seek consent in circumstances where research subjects are contactable but the process of seeking consent would damage the scientific integrity of the proposed research. In addition, if a research participant previously has given consent in general terms for their health information to be used in a future similar research study, even though it may not be 'impracticable' to seek specific consent for the second study it may be quite unnecessary and inefficient to do so.[105]

65.93 The OPC Review noted evidence that requiring consent to participate in some research projects significantly reduces the participation rate—and therefore the scientific value and integrity of the research.[106] The AIC stated that in criminal justice research, consent can raise complex bias issues:

> For example, a study that attempts to understand the correlates of delinquent behaviour amongst a sample of primary school children requires the permission of parents for their children to answer the questionnaire. However, parents whose children are less likely to be engaged in delinquent activity might be more likely to give consent, consequently biasing the sample. This would affect the validity of the results resulting in poor, and possible harmful, policy and practitioner responses.[107]

ALRC's view

65.94 The ALRC has considered the arguments put forward in relation to 'impracticable to seek consent' and acknowledges that 'impracticable' may not be the clearest and most appropriate test in some circumstances. For example, it may be practicable to obtain consent from individuals to use their personal information for the purposes of research in the sense that it is logistically possible, but obtaining their consent may have an unacceptable adverse impact on the integrity and validity of the research. The term 'impracticable', as defined above, does place a certain emphasis on the means of obtaining consent, rather than the impact of obtaining consent.

65.95 The Section 95 Guidelines incorporate a reasonableness test in relation to agencies—that is, research may proceed without consent when it is reasonable to do so. While it might be practicable to seek the consent of research participants in a particular case, it would not be reasonable to do so if this would have an unacceptable adverse impact on the integrity and validity of the research.

65.96 Both these tests should be picked up and incorporated in the model UPP research exceptions. The ALRC recommends, therefore, that agencies and organisations should be able to collect, use or disclose personal information for the

---

104 General Ethical Issues Sub-Committee—Alfred Hospital Ethics Committee, *Submission PR 531,* 21 December 2007.

105 National Health and Medical Research Council, *Submission PR 397,* 7 December 2007.

106 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.

107 Australian Institute of Criminology, *Submission PR 461,* 12 December 2007.

purposes of research without consent where it is 'unreasonable or impracticable' to seek that consent.

65.97 This test is mirrored in the 'Collection' principle, which requires that where it is 'reasonable and practicable' personal information about an individual must be collected from that individual.

65.98 It is important to note that 'unreasonable or impracticable to seek consent' is only one element of the research exceptions. All of the other safeguards set out in the exceptions would apply, including the requirement that an HREC be satisfied that the public interest in the research outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*. In addition, the research would have to be conducted in accordance with the Research Rules issued by the Privacy Commissioner.

Recommendation 65–5 The research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle should include a provision stating that it must be 'unreasonable or impracticable' to seek consent from individuals to the collection, use or disclosure of their personal information before that information may be used without consent for the purposes of research.

Human Research Ethics Committees

Role of HRECs

65.99 Institutions that undertake research 'with or about people, their data or tissue'[108] are responsible for ensuring that research they conduct, or for which they are responsible, is ethically reviewed in accordance with the National Statement.[109] Institutions may establish their own processes for ethical review or use those of another institution.[110]

65.100 The National Statement provides that ethical review can be undertaken at various levels depending on the degree of risk involved in the research. Research involving 'negligible risk' and the use of existing collections of data or records that contain only non-identifiable information may be exempt from review.[111] Research

108 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), 8. This is the definition of 'human research' used in the National Statement.
109 Ibid, [5.1.1].
110 Ibid, [5.1.3].
111 Ibid, [5.1.22].

involving 'no more than a low level of risk' may be reviewed by a non-HREC ethical review body,[112] such as a departmental committee, or a subcommittee of an HREC.[113] Research involving more than a low level of risk must be reviewed by an HREC. The National Statement expressly provides that research proposing to use personal information in medical research without consent and research using health information without consent must be reviewed by an HREC.[114] These provisions reflect the existing exceptions for research under the IPPs and NPPs.

65.101 HRECs must be composed and function in accordance with the National Statement.[115] The minimum membership of an HREC is eight: a chairperson; at least two lay people (one man and one woman) who have no affiliation with the institution; at least one person with knowledge of, and experience, in the professional care, counselling or treatment of people; at least one person who performs a pastoral care role in the community; at least one lawyer; and at least two people with current research experience.[116] The primary responsibility of HREC members is to decide whether a proposal meets the requirements of the National Statement and is ethically acceptable.[117]

65.102 Both the Section 95 and 95A Guidelines provide a detailed framework within which HRECs must consider the privacy implications of research proposals involving the use of individuals' personal or health information. In particular, HRECs must consider, and may approve, research proposals seeking to use personal or health information without consent, on the basis that the public interest in the research substantially outweighs the public interest in maintaining the level of privacy protection provided by the IPPs and the NPPs.

65.103 The Guidelines require that, before making a decision, an HREC must assess whether it has sufficient information, expertise and understanding of privacy issues, either among the members of the HREC or otherwise available to it, to make a decision that takes proper account of privacy.[118] The Section 95A Guidelines note that it may be necessary to appoint additional members with specific expertise in some circumstances. It is important to note that, although an HREC may give approval for a research proposal to proceed, the final decision to release personal information to researchers is not made by an HREC, but by the relevant data custodian.

---

112 Ibid, [5.1.7].
113 Ibid, [5.1.20].
114 Ibid, [2.3.5].
115 Ibid, Ch 5.1.
116 Ibid, [5.1.30].
117 Ibid, [5.2.2].
118 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.1]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [D.1].

Discussion Paper proposals

65.104 In IP 31, the ALRC asked whether HRECs are the most appropriate bodies to make decisions about the collection, use and disclosure of personal information without consent in the context of health and medical research.[119] In DP 72, the ALRC reported that there was widespread support for the role of HRECs in this area and expressed the view that HRECs remain the most appropriate bodies to make decisions about the collection, use and disclosure of personal information without consent in the research context. The ALRC proposed that, as review and approval by HRECs was an important safeguard around the use of personal information in research, the role of HRECs should be set out expressly in the research exceptions to the UPPs.[120] In addition, the ALRC proposed that the National Statement should be amended to require that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by an HREC.[121]

Submissions and consultations

65.105 In its submission to IP 31, the NHMRC originally urged

> the ALRC to reconsider the role of HRECs in decisions about the privacy implications of the collection, use or disclosure of health information in research. The NHMRC is of the view that these considerations could be managed without intervention by an HREC although we have not identified a replacement mechanism at this stage.[122]

65.106 Having asked the ALRC to reconsider the issue, however, the NHMRC also submitted that HRECs are, in general, appropriately constituted to enable them to perform the role assigned to them under the *Privacy Act* and Section 95 and 95A Guidelines. In its submission to DP 72, the NHMRC supported the ALRC's proposals in this area, stating that:

> We support the proposed continuing role of Human Research Ethics Committees (HRECs) in reviewing and approving research proposals that seek to rely on the research exceptions in the *Privacy Act*, but note that resource and capacity implications for HRECs will need to be evaluated.[123]

65.107 On the other hand, Professor Thomson was strongly of the view that the function of HRECs is to assess whether research projects are ethically acceptable, not whether research projects conform with legal requirements:

---

119 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–31.
120 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–4.
121 Ibid, Proposal 58–6.
122 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
123 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

> The proposal to maintain reliance on HRECs as agents in the application of part of the statutory privacy regime will continue a role and responsibility that has proved foreign and burdensome.[124]

65.108 He noted, for example, that the Section 95A Guidelines impose responsibility on HRECs to decide whether a particular research proposal is consistent with the NPPs, including whether it is 'impracticable to seek consent'. He noted that often it is organisations that hold personal information—rather than individual researchers—that are responsible for seeking consent and that, as HRECs do not have a direct relationship with such organisations, they are not in a strong position to evaluate whether it is impracticable for the organisation to do so.[125]

65.109 A number of others raised concerns about the role of HRECs under the *Privacy Act*. The University of Newcastle stated that data custodians and the Privacy Commissioner should take more responsibility for determining when it is appropriate to collect, use and disclose personal information without consent for research. The University also noted that the National Statement provides that 'compliance with legal obligations (statutory or otherwise) … is not within the scope of the National Statement'. The University commented that, if HRECs are to have a continuing role under the *Privacy Act*, the National Statement will need to address those legal requirements.[126]

65.110 There was strong support, however, from other stakeholders for the role of HRECs in reviewing research proposals under the *Privacy Act*.[127] The Centre for Law and Genetics stated that:

> We are strongly of the view that Human Research Ethics Committees are the most appropriate bodies to make decisions about the collection, use and disclosure, without consent, of health information in the context of health and medical research. This model of ethical review, based on the collective wisdom of an interdisciplinary group, has proved in general to be very effective in practice.[128]

---

124 C Thomson, *Submission PR 454*, 7 December 2007.

125 Ibid.

126 University of Newcastle, *Submission PR 413*, 7 December 2007.

127 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Australian Institute of Criminology, *Submission PR 461*, 12 December 2007; Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007; CSIRO, *Submission PR 176*, 6 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006; Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

128 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

65.111 The Centre for Law and Genetics also expressed support for the recommendations relating to HRECs in ALRC 96.[129] The Caroline Chisholm Centre for Health Ethics noted the need for adequate funding, training and education of HRECs and their members.[130]

65.112 The OPC submitted that HRECs are the most appropriate bodies to make decisions about the collection, use and disclosure of health information without consent in the health and medical research context.[131] The OPC agreed that the National Statement should be amended to specify that, where a research proposal seeks to rely on the research exceptions in the Act, it must be reviewed and approved by an HREC.[132] A number of other major stakeholders expressed similar views.[133]

ALRC's view

65.113 The ALRC has considered the role of HRECs in the privacy regime and notes that, while some concerns have been expressed, there was significant support for the role HRECs currently play under the *Privacy Act*. HREC review provides a valuable safeguard by considering on a case-by-case basis research proposing to collect, use or disclose identified or reasonably identifiable personal information without consent. Research involving the use of personal information without consent raises ethical as well as privacy issues, and the vast majority of stakeholders commenting on this issue in this Inquiry considered that HRECs are well placed to consider these issues.

65.114 The role and responsibilities of HRECs and other parties involved in human research under the *Privacy Act* and the Section 95 and 95A Guidelines, however, have become somewhat confused. The research exceptions to the model UPPs, recommended below, will go some way to clarifying the role of HRECs in this process. HRECs should not be responsible for ensuring that research proposals meet all the legal requirements in the *Privacy Act.* Organisations and agencies that collect, use or disclose personal information without consent for the purposes of research are responsible for ensuring that those activities are conducted in a way that complies with the Act and with any rules issued by the Privacy Commissioner under the research exceptions.

---

129 Ibid.

130 Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

131 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

132 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

133 Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

65.115 The research exceptions set out below require HRECs to review such activities and decide whether the public interest in the proposed activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*. In considering this balance, the ALRC anticipates that HRECs will focus on factors such as the value and public importance of the research; the risk of harm to individuals; the standards of conduct that are to be observed in the research; and the extent of any possible breach of privacy.

65.116 Although other elements of the research exceptions—for example, that it must be unreasonable or impracticable to seek consent—are distinct from HREC review of the public interest, it may be necessary for HRECs to consider how these elements impact on the public interest balance. For example, an HREC may need to consider the extent to which seeking consent would impact on the scientific value and integrity of the research. If there is unlikely to be a significant impact on the value and integrity of the research then the public interest may well dictate that the agency or organisation be required to seek consent for the collection, use or disclosure of the information. It is not the responsibility of HRECs, however, to certify that it is unreasonable or impracticable to seek consent in any particular case.

65.117 HRECs may also have to consider the extent to which the proposed collection, use or disclosure complies with the Research Rules to be issued by the Privacy Commissioner, in order to decide where the public interest balance lies. But the Research Rules should target agencies and organisations that collect, use or disclose personal information in the course of research, rather than HRECs. It is these agencies and organisations that have responsibility to ensure that their conduct complies with the *Privacy Act*.

65.118 The National Statement and its oversight mechanisms, including review by HRECs, is not limited to health and medical research, but is intended to cover all research involving humans. The ALRC recommends, above, extending the existing arrangements relating to the collection, use and disclosure of personal information in health and medical research to include the collection, use or disclosure of personal information in research involving humans more generally. HRECs should be required to review and approve all such activities.

65.119 The National Statement currently provides that only an HREC may approve research that proposes to use personal information without consent in medical research, or personal health information without consent.[134] In addition, the National Statement provides that only an HREC may approve research that involves more than a low level of risk.[135] In the context of extending the arrangements for research under the *Privacy Act*, the National Statement may also require amendment. Any research that requires:

---

134 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [2.3.5].

135 Ibid, 8.

- the collection of identified or reasonably identifiable sensitive information without consent;

- the use or disclosure of such information without consent for a purpose that is not directly related to the purpose of collection and within the reasonable expectations of the individual; or

- the use or disclosure of identified or reasonably identifiable non-sensitive information without consent for a purpose that is not related to the purpose of collection and within the reasonable expectations of the individual,

is likely to involve more than a low level of risk for individuals and always should be reviewed by an HREC. In these circumstances, researchers and data custodians will be relying on the research exceptions in the 'Collection' principle and the 'Use and Disclosure' principle, discussed further below. The ALRC recommends, therefore, that the National Statement be amended to require that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by an HREC.

Recommendation 65–6 The National Health and Medical Research Council, the Australian Research Council and Universities Australia should amend the *National Statement on Ethical Conduct in Human Research* to state that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by a Human Research Ethics Committee.

Accountability of HRECs

65.120 The Section 95 and 95A Guidelines also require HRECs to record their decisions, including details of the agency or organisation from which information will be sought, the information sought, the number of records involved, and the IPP or NPP likely to be infringed.[136] The Australian Health Ethics Committee (AHEC) is, in turn, required to report annually to the NHMRC in relation to HRECs generally, and to provide a compliance report setting out decisions taken by HRECs under the

136 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.4]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [D.6].

Guidelines.[137] AHEC is also required to provide the compliance report to the Privacy Commissioner[138] and to report where there has been a breach of the Guidelines.[139]

65.121 Submissions to the OPC Review suggested that the reporting obligations imposed on HRECs by the guidelines are unnecessarily onerous—for example, the requirement to list those IPPs and NPPs that may be breached by the research proposal.[140] The OPC Review considered this issue and made the following recommendation:

> The Office will work with the National Health and Medical Research Council to simplify the reporting process for human research ethics committees under the section 95A guidelines.[141]

65.122 In IP 31, the ALRC asked whether the requirements imposed on HRECs by the Section 95 and 95A Guidelines were appropriate and effective.[142] In response, the NHMRC expressed concern about the reporting requirements. The NHMRC noted that the complexity of the regulatory regime and the detailed reporting requirements have resulted in an excessive administrative burden. The NHMRC suggested a reporting framework that involved less detailed, commentary-based reporting on privacy issues that arise during a reporting period, and an exception-based reporting framework for specific privacy concerns that come to the attention of HRECs during a reporting period.[143]

65.123 In DP 72, the ALRC agreed with the OPC Review that the Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements imposed on AHEC and HRECs. The ALRC proposed that any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.[144]

---

137 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [4.1]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [E.1].

138 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [5.1]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [F.1].

139 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [4.3]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [E.3].

140 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004; University of Western Australia Human Research Ethics Committee, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004.

141 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 62.

142 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–32.

143 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

144 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–7.

Submissions and consultations

Reporting

65.124 The Alfred Hospital Ethics Committee noted difficulties in meeting the current reporting requirements and strongly supported the ALRC's proposal[145] that there should be a review.[146] Other stakeholders also expressed support for a review and for the ALRC's proposed framework for any new reporting mechanism.[147]

65.125 The OPC agreed that a review was appropriate and reiterated that it would work with the NHMRC to simplify the reporting requirements under the Section 95 and 95A Guidelines.

> The Office recognises the importance of ensuring that reporting requirements are not burdensome, do not hinder the operation of HRECs or impose unreasonable compliance costs. In the Office's view … these reporting requirements should include only as much information as is necessary to ensure that there is transparency in how the research exceptions are being used. Such transparency, in turn, will help promote community trust and confidence in non-consensual handling of personal information for research.[148]

65.126 The OPC submitted that, in order to promote transparency and community confidence, reports on HREC consideration of research proposing to proceed under the research exceptions should be made public.[149]

Review of decisions?

65.127 A further issue raised by stakeholders in relation to the accountability of HRECs, was whether the decisions of HRECs under the research exceptions in the *Privacy Act* should be subject to some form of review. National Legal Aid stated that:

> If research ethics committees are to continue to serve as the primary mechanism for approving research where it is impracticable to obtain subject consent, there should be greater accountability in the way decisions are reached. This would be assisted by better thought out and more detailed reporting requirements for ethics committees.

---

145 Ibid, Proposal 58–7.

146 General Ethical Issues Sub-Committee—Alfred Hospital Ethics Committee, *Submission PR 531*, 21 December 2007.

147 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

148 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

149 Ibid.

> Accountability could also take the form of affected people having the ability to seek Privacy Commissioner review of ethics determinations.[150]

65.128 The Law Society of New South Wales also suggested that decisions of HRECs on the balance of public interest should be subject to appropriate review mechanisms.[151] The New South Wales Council for Civil Liberties expressed the view that where information was to be used without consent, this should be approved by the Privacy Commissioner and an HREC.[152]

65.129 The OPC supported elevating the requirement for HREC review from the Section 95 and 95A Guidelines into the *Privacy Act*.[153] Professor Thomson, however, was concerned that this may have undesirable consequences, such as increasing concern among HREC members about the legal consequences of their decisions, leading to more conservative decision making. He also asked whether this would result in HREC decisions becoming subject to judicial review.[154]

ALRC's view

Reporting

65.130 The ALRC notes that the Privacy Commissioner is committed to reviewing the reporting requirements currently imposed on HRECs and on AHEC by the Section 95 and 95A Guidelines. Any reporting requirements should have clear goals and should impose the minimum possible administrative burden to achieve those goals. This might be achieved, for example, by minimal first tier reporting of the number of proposals considered and the number approved and rejected, while allowing for follow-up by the Privacy Commissioner if these reports raised concerns or indicated undesirable trends.

65.131 The ALRC supports initiatives by the Privacy Commissioner and the NHMRC to review reporting requirements under the existing arrangements. If the *Privacy Act* is amended as recommended in this Report, it will be necessary to consider whether to impose a formal reporting requirement on HRECs. The ALRC sees merit in a simplified reporting regime and the publication of periodic report results in order to encourage transparency and public awareness. A regime under which periodic reports are made to the Privacy Commissioner will allow the Commissioner to assess the extent of the use of personal information without consent for research and will allow the Commissioner to intervene, for example, by conducting an investigation, if undesirable trends become apparent.

---

150 National Legal Aid, *Submission PR 521*, 21 December 2007.
151 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.
152 New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007.
153 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
154 C Thomson, *Submission PR 454*, 7 December 2007.

65.132 These reports should be made public, and the ALRC notes that some past reports have been published by the NHMRC.[155] In addition, the National Statement provides that research institutions should publish descriptions of all research projects in which an HREC has approved the use of personal information without consent.[156]

Review

65.133 The accountability of the HREC system was considered in detail in ALRC 96,[157] prompted in part by the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into human cloning and stem cell research.[158] In ALRC 96, the ALRC and AHEC recommended that there be independent auditing of HREC processes and standardised record keeping and reporting arrangements.[159] The ALRC remains of the view that periodic, well structured, transparent reporting is one way of providing effective oversight of HREC decision making under the *Privacy Act*.

65.134 The ALRC considered the concern that elevating the requirement for review by an HREC from the Section 95 and 95A Guidelines into the *Privacy Act* may mean that those decisions become subject to judicial review.[160] In the ALRC's view, this change alone is unlikely to mean that members of HRECs will be characterised as 'officers of the Commonwealth'—unless they already happen to be 'officers of the Commonwealth' in some other capacity—so as to give rise to a right of judicial review under s 75(v) of the *Australian Constitution*, or s 39B of the *Judiciary Act 1903* (Cth).

65.135 HRECs are institutional, rather than statutory committees, established on an administrative basis in accordance with the National Statement. Members are generally volunteers, drawn from a range of community sectors. At least one third of the

---

155 National Health and Medical Research Council, *Report of the 2002–03 HREC Annual Report Process* (2004).

156 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [2.3.8].

157 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Ch 17.

158 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Human Cloning: Scientific, Ethical and Regulatory Aspects of Human Cloning and Stem Cell Research* (2001).

159 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 17–1.

160 Judicial review is to be distinguished from merits review. Judicial review of an administrative decision involves a court reviewing the legality of the process followed to make the decision, not the substance of the decision (merits review). The *Administrative Decisions (Judicial Review) Act 1977* (Cth) provides an aggrieved person—that is, someone whose rights or interests are affected by a decision—with broad grounds to apply for review. These grounds include: a breach of the rules of natural justice; that the decision was induced or affected by fraud; that there was no evidence or other material to justify the making of the decision; and that the making of the decision was an improper exercise of power. The latter includes: taking an irrelevant consideration into account; failing to take a relevant consideration into account; exercising a discretionary power in bad faith; and unreasonableness.

members of an HREC are required to be from outside the institution for which the HREC is reviewing research, including two lay people who have no affiliation with the institution.[161] Even where an HREC is established by a public sector agency, therefore, the committee is not composed entirely of officers of that agency. Members are asked to make decisions on the basis of their own judgement.[162]

65.136 The ALRC also considered whether decisions of HRECs under the *Privacy Act* could be characterised as decisions 'of an administrative character made, proposed to be made, or required to be made (whether in the exercise of a discretion or not…) … under an enactment' for the purposes of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (ADJR Act).[163] The ADJR Act provides a right to apply to the Federal Court of Australia or the Federal Magistrates Court for judicial review of such decisions.[164]

65.137 This issue would arise whether the requirement for HREC review was included in the provisions of the *Privacy Act*, or in the Research Rules to be issued by the Privacy Commissioner. The ALRC intends that the Research Rules, and any other rules issues by the Privacy Commissioner, should be legislative instruments for the purposes of the *Legislative Instruments Act 2003* (Cth).[165] An 'enactment' for the purposes of the ADJR Act includes 'an instrument (including rules, regulations or by-laws) made under such an Act'. Thus, a decision under the *Privacy Act* or a decision under the Research Rules is likely to amount to a decision 'under an enactment'.

65.138 In any event, it is appropriate to include the requirement for HREC review in the Act itself. HREC review is a fundamental element of the research exceptions and should be included in the Act for reasons of transparency.

65.139 Traditionally, the principles of administrative law—including judicial review of administrative decisions—applied only to government decision makers. As noted by Justice Michael Kirby in a paper delivered in 2006, however, both the public sector and government service delivery in Australia have fundamentally changed in the past 30 years.

> The lines between the public and private sectors are becoming increasingly blurred. Such changes have highlighted significant tensions and gaps in administrative law, in Australia and elsewhere. They have raised important questions as to the development of the law in this area … To what extent should administrative law be applied to

161 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [5.1.30].
162 Ibid, [5.2.2].
163 *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 3.
164 Ibid ss 3, 5, 6.
165 See discussion of the status of binding rules issued by the Privacy Commissioner in Ch 47.

> private or hybrid bodies, when those bodies are exercising responsibilities of a public nature?[166]

65.140 Justice Kirby is of the view that where a private body is exercising public power—where decisions are 'being made on behalf of the people'—public accountability, including before the courts, is entirely appropriate.[167] The state of the law in this area, however, is not settled. In *Neat Domestic Trading Pty Ltd v AWB Ltd*,[168] the majority (McHugh, Hayne and Callinan JJ) declined to answer the question whether public law remedies can be granted against private bodies in circumstances of this kind. The majority confined their decision to the legislative features of the case, holding that public law remedies did not lie against the respondent decision maker because of the particular structure of the relevant statutory provisions, the 'private' character of the respondent as a company incorporated under companies legislation with a profit-making objective, and the incompatibility of the respondent's private interests and public law obligations.

65.141 Kirby J, in dissent, argued that the fact the decision maker was a private company was of no immediate legal consequence.[169] The statutory scheme under consideration had entrusted decisions of a public, regulatory character to a private company, involving that body in the exercise of public power. In Kirby J's view, these decisions were of an administrative character made under an enactment and, in the circumstances of the case, amenable to review under the ADJR Act. Gleeson CJ held that it was unnecessary to decide whether the decisions of the company were of 'an administrative character made under an enactment', but indicated a preference for the view that they were—with the result that they would be subject to review under the ADJR Act.

65.142 The case is not authority for the proposition that the decisions of private bodies cannot be subject to public law remedies, but it does show that the law in this area is uncertain and its growth incremental. The case indicates that a majority of the High Court is cautious about extending public law remedies to the decisions of private bodies, notwithstanding that the decisions have a public aspect.

65.143 Factors that might be taken into account by the courts include the nature of HREC membership and decision-making process. As noted above, members are generally volunteers, appointed in their personal capacity, and not as representatives of any organisation, group or opinion.[170] The HREC review process is not intended to be

---

166 M Kirby, 'Public Funds and Public Power Beget Public Accountability' (Paper presented at Corporate Governance in the Public Sector Conference, Canberra, 9 March 2008), 4.

167 Ibid, 5.

168 *Neat Domestic Trading Pty Ltd v AWB Ltd* (2003) 216 CLR 277.

169 Ibid, 315.

170 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [5.1.30].

adversarial, but rather an iterative process in which there is room for negotiation and ongoing amendment and refinement of research proposals.[171] Notwithstanding that *Neat Domestic Trading Pty Ltd v AWB Ltd* does not say a great deal about the general availability of public law remedies, at least part of the majority's reasoning is strongly supportive of an argument that the imposition of public law obligations on an HREC would be inconsistent with this kind of community-based, iterative process.

65.144 Given the three–two split in the court, it is possible that the law will develop in such a way that HREC decisions under the *Privacy Act* come to be characterised as decisions 'of an administrative character made under an enactment'. It would then become necessary to consider options such as providing an exemption from judicial review for HREC decisions by regulation,[172] or substantially restructuring the decision-making process under the research exceptions to the *Privacy Act.*

Recommendation 65–7 The Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements imposed under the *Privacy Act* on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.

HRECs: Composition and decision making

65.145 Other issues identified in the course of the OPC Review included the tendency of HRECs to make 'conservative' decisions, and the need to involve a number of HRECs in relation to some research proposals, particularly national proposals.[173] Concern was expressed about inconsistencies in the way HRECs balance the public interests in research and privacy,[174] and in relation to the membership of HRECs.[175] Similar issues were raised in the course of the current Inquiry.[176]

65.146 In ALRC 96, the role and function of HRECs in the context of genetic research were considered in detail, and a range of recommendations to improve HREC decision making and to support HRECs in their work were made. In particular, the ALRC and AHEC recommended that:

---

171 Ibid, [5.2.13].

172 *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 19.

173 University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

174 South Australian Government Department of Health, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

175 University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

176 B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006.

> The National Health and Medical Research Council (NHMRC) should develop and implement procedures to promote consistency, efficiency, transparency and accountability in the review of human genetic research by Human Research Ethics Committees (HRECs). In developing such procedures, the NHMRC should initiate a systematic quality improvement program that addresses:
>
> - consolidation of ethical review by region or subject-matter;
> - the membership of HRECs and, in particular, the balance between institutional and non-institutional members;
> - the need for expertise of HRECs in considering proposals for human genetic research;
> - on-going monitoring of approved human genetic research projects;
> - the education and training of HREC members;
> - payment of HREC members for their work in reviewing research proposals;
> - independent audit of HREC processes; and
> - standardised record keeping and reporting to the NHMRC, including in relation to commercial arrangements.[177]

65.147 The ALRC and AHEC also recommended that:

> The NHMRC, in strengthening the level of training and other support provided to HRECs … should ensure that adequate attention is given to: (a) the interpretation of the waiver of consent provisions of the National Statement; and (b) HREC decision making in relation to such waiver.[178]

65.148 A number of initiatives are under way to address these issues. First, the National Statement has been revised extensively and redrafted.[179] In addition, the Australian Government provided the NHMRC, in the 2007 federal budget, with $5.6 million over four years to replace multiple ethics review of research projects with a single national approach. The proposed system will streamline approval of cross-jurisdictional and multi-centre research by establishing national committees to conduct a single review of such research. These committees will be established in consultation with states and territories.[180]

---

177 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 17–1.

178 Ibid, Rec 15–3.

179 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

180 Australian Government Department of Health and Ageing, *Health and Medical Research—Streamlining Human Research Ethics Reviews* (2007) <www.health.gov.au/budget2007> at 27 August 2007.

65.149 The New South Wales Department of Health has developed its own model of single ethical review of multi-centre research in the New South Wales public sector. The model was implemented on 1 July 2007.[181] The Victorian Government Department of Human Services is also working on a project to implement a centralised system of ethical review for multi-centre research.[182]

65.150 The CSIRO submitted that:

> A key development in removing impediments to such multi-centre research has been the National Ethics Application Form (NEAF)13, available for public use since May 2006. This Application Form is an electronic, web based form for use by researchers in any research discipline when submitting research proposals to one or more Human Research Ethics Committee (HREC) for review.[183]

65.151 Given these recent comprehensive reviews and developments, the ALRC does not propose to reconsider the HREC decision-making process in detail in this Report. The ALRC notes developments in relation to the harmonisation and simplification of ethical review and the development of a National Ethics Application Form. The ALRC recommends, above, that the Section 95 and 95A Guidelines should be replaced by a single set of Research Rules issued by the Privacy Commissioner.[184] The adoption of a single set of UPPs and a single set of rules relating to research, to be developed in consultation with stakeholders, will have a significant impact on reducing regulatory complexity and the regulatory burden on HRECs.

Research exceptions to the model Unified Privacy Principles

65.152 Part D of this Report recommends a set of model UPPs. In this section the ALRC recommends exceptions to the 'Collection' principle and the 'Use and Disclosure' principle to allow research using identified or reasonably identifiable personal information without consent to proceed, where the public interest in allowing the research to go forward outweighs the public interest in maintaining the level of privacy protection provided by the UPPs.

65.153 Currently, NPP 10.3 provides, in part, that health information may be collected without consent where necessary for research, or the compilation or analysis of statistics, where:

- it is relevant to public health or public safety;

---

181 New South Wales Government Department of Health, *NSW Health Model for Single Ethical and Scientific Review of Multi-Centre Research* (2007) <www.health.nsw.gov.au/healthethics/multicentre_research.html> at 27 August 2007.

182 Victorian Government Department of Human Services, *Streamlining Ethical Review of Multi-Centre Research in Victoria* (2007) <www.health.vic.gov.au/ethics/multi/index.htm> at 27 August 2007.

183 CSIRO, *Submission PR 176*, 6 February 2007.

184 Rec 65–1.

- the purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained;

- it is impracticable for the organisation to seek the individual's consent to the collection; and

- the information is collected as required by law; or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or in accordance with guidelines approved under s 95A.

65.154 In addition, NPP 10.4 provides that if an organisation collects health information about an individual in accordance with NPP 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

65.155 NPP 2.1(d) provides that an organisation may use or disclose health information without consent where necessary for research, or the compilation or analysis of statistics, where:

- it is relevant to public health or public safety;

- it is impracticable for the organisation to seek the individual's consent before the use or disclosure;

- the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under s 95A; and

- in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose that information, or personal information derived from that information.

Discussion Paper proposals

65.156 In DP 72 the ALRC proposed that a similar regime should be established under the model UPPs, applying to agencies and organisations, with the following modifications.

65.157 The 'Collection' principle expressly allows the collection of sensitive information without consent where the collection is required or authorised by or under law. It was not necessary, therefore, to include this specifically in the provision dealing with collection of sensitive information for research. In addition, and as discussed in Chapter 63, the OPC is not aware of any existing rules established by competent health

or medical bodies that would fulfil the requirements of NPP 10.3. Consequently, the ALRC omitted the references to these two mechanisms from the proposed research exceptions. Instead, the research exceptions provided that personal information could be collected, used and disclosed without consent where necessary for research if all of the following conditions were met:

- the purpose could not be served by the collection of information that did not identify the individual;
- it was impracticable for the agency or organisation to seek the individual's consent;
- an HREC was satisfied that the public interest in the activity outweighed the public interest in maintaining the level of privacy protection provided by the UPPs; and
- the information was collected, used and disclosed in accordance with rules to be issued by the Privacy Commissioner.

65.158 The Section 95 and 95A Guidelines are issued by the NHMRC and approved by the Privacy Commissioner. Once approved and gazetted the guidelines become binding. Because of the recommendation to expand the scope of the research exception beyond health and medical research to apply to human research generally,[185] the ALRC indicated that it was no longer appropriate to rely on the NHMRC alone to develop guidelines for the conduct of research. The ALRC proposed that the research exceptions to the model UPPs simply provide that the rules to guide the conduct of research should be issued by the Privacy Commissioner, who would consult with stakeholders, including the authors of the National Statement, in developing the rules.

65.159 In contrast to NPP 1, the 'Collection' principle deals with the collection of both sensitive and non-sensitive information. The 'Collection' principle does not require consent for the collection of non-sensitive information and so the research exception was limited to the collection of sensitive information.

65.160 The ALRC also proposed that NPP 10.4 should be re-worded so that the provision no longer required that reasonable steps be taken to 'permanently de-identify' information before it is disclosed. It is sufficient to require agencies and organisations that collect sensitive information under the research exception to take reasonable steps to ensure that the information is not disclosed in a form that would identify individuals or from which individuals would be reasonably identifiable. This approach is more consistent with the definition of 'personal information' discussed in Chapter 6.[186] Where information is not about an identified or reasonably identifiable

185 Rec 65–2.
186 Rec 6–1.

individual, it will not fall within the recommended definition of 'personal information' and will no longer be covered by the *Privacy Act*.

Submissions and consultations

65.161 The AIC strongly supported the ALRC's proposed research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle.[187] Other stakeholders also expressed support.[188] PIAC expressed qualified support for the exceptions, but was concerned about the use of the word 'reasonable' in the context of taking 'reasonable' steps to ensure that information is not disclosed in a form that would identify individuals or from which individuals would be reasonably identifiable. PIAC also questioned the use of the phrase 'reasonably believes', in the context of an agency or organisation 'reasonably believing' that the recipient of personal information will not disclose the information in a form that would identify individuals, or from which individuals would be reasonably identifiable.[189]

65.162 The OPC agreed with some elements of the proposed research exceptions but, as discussed above, did not support: expanding the exceptions to include human research generally; requiring the Privacy Commissioner to issue the Research Rules; or amending the public interest test from 'substantially outweighs' to 'outweighs'.[190]

ALRC's view

65.163 It is appropriate to require agencies and organisations that have collected personal information for research purposes to take 'reasonable steps' to ensure that it is not possible to identify individuals from their published results. Reasonable steps might include, for example, applying techniques—employed by the ABS and other agencies, and discussed in Chapter 6—such as data suppression, data rounding and category collapsing. While these techniques minimise the risk that individuals will be identifiable, it is not always possible to ensure absolutely that no-one will be able to identify individual involved. In these circumstances, it would be inappropriate to impose absolute liability on agencies and organisations to ensure that information is not disclosed in an identifiable form.

65.164 It is also appropriate to impose a requirement that agencies and organisations 'reasonably believe' that the recipient of the personal information will not disclose the information in an identifiable form. Where agencies and organisations are not, themselves, in control of personal information because it has been disclosed to a

187 Australian Institute of Criminology, *Submission PR 461*, 12 December 2007.
188 Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007.
189 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
190 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

researcher for use in a research project, for example, it is not possible for those agencies and organisations to ensure absolutely that the researcher will handle the information appropriately. On the other hand, the agency or organisation should be required to have a reasonable belief that this will occur. A 'reasonable belief' cannot be without foundation, and the agency or organisation would have to be able to indicate those factors that provided the basis for the belief—for example: the good reputation and past best practices of the researcher; and the arrangements put in place between the agency or organisation and the researcher to ensure that the information was handled appropriately.

65.165 The following recommendations set out the elements the ALRC considers should be included in the research exceptions to the UPPs.

Recommendation 65–8 The research exception to the 'Collection' principle should provide that an agency or organisation may collect personal information, including sensitive information, about an individual where all of the following conditions are met:

(a) the collection is necessary for research;

(b) the purpose cannot be served by the collection of information that does not identify the individual;

(c) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;

(d) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; and

(e) the information is collected in accordance with the Research Rules, to be issued by the Privacy Commissioner.

Where an agency or organisation collects personal information about an individual under this exception, it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Recommendation 65–9 The research exception to the 'Use and Disclosure' principle should provide that an agency or organisation may use or disclose personal information where all of the following conditions are met:

(a) the use or disclosure is necessary for research;

(b) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;

(c) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*;

(d) the information is used or disclosed in accordance with the Research Rules, to be issued by the Privacy Commissioner; and

(e) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable.

66. Research: Databases and Data Linkage

Contents

Introduction

66.1 Databases and registers of health information are established for a number of reasons in both the health services and the health and medical research contexts. The National Health Information Management Group has defined a 'health register' as follows:

> For the purposes of these guidelines, a health register is a collection of records containing data about aspects of the health of individual persons. The subjects will typically be patients or clients of a health service or health program, from which the data are collected. Health registers are characterised by being:
>
> *personal data* each record represents a person, not a set of aggregated data;
>
> *identified* each record in the register is identified to a particular subject;
>
> *population-based* the register aims to include a record of all persons within its defined scope; populations may be broadly or narrowly defined, eg Australia wide, regionally based or clients of a local service; and
>
> *ongoing* collection is not restricted to a particular period of time.[1]

1 Australian Institute of Health and Welfare, *Minimum Guidelines for Health Registers for Statistical and Research Purposes* (2001), 2.

66.2 Dr Roger Magnusson defines health registers as 'discrete repositories of information separate from clinical records' but notes that the distinction between clinical records and data registers is likely to diminish as health records are gradually incorporated into databases.[2] The establishment and management of electronic health information systems and shared electronic health records in the health services context are discussed in Chapter 61. This chapter will focus on the establishment and use of health information databases and registers in the research context.

Establishing databases

Background

66.3 A number of health information databases and registers have been established by legislation—for example, the Australian Government maintains the Medicare and Pharmaceutical Benefits Program databases. State and territory governments in Australia have established databases that include information collected under mandatory reporting requirements in public health legislation. For example, the *Public Health Act 1991* (NSW) requires health service providers to notify the cervical cancer register of cervical cancer screening tests performed and the results of those tests. The Act states that the purpose of the register is to reduce the incidence of, and mortality from, preventable cervical cancer.[3]

66.4 A wide range of non-statutory databases collect information on a voluntary basis and may be established and maintained by hospitals, universities, research bodies and others. For example, the Australian and New Zealand Dialysis and Transplant Registry (ANZDATA) records the incidence, prevalence and outcome of dialysis and transplant treatment for patients with end stage renal failure.[4] The Menzies Centre for Population Research maintains a research database comprising extensive genealogical data, genetic samples, and health information supplied by donors, to search for genetic causes of disease. All material is provided with consent specifically for the Centre's research projects.

66.5 Health service providers, such as hospitals, also maintain extensive databases established in the course of delivering health services and for management, funding and monitoring purposes.

66.6 In its submission to the Office of the Privacy Commissioner's (OPC) review of the private sector provisions of the *Privacy Act* (the OPC Review), the National Health and Medical Research Council (NHMRC) noted that access to health information in such registers is crucial to the conduct of public health research but expressed concern

---

2 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 15.

3 *Public Health Act 1991* (NSW) s 42G.

4 ANZDATA is located at The Queen Elizabeth Hospital in South Australia.

that the *Privacy Act* does not provide an appropriate regime for the establishment, maintenance and use of such registers.[5]

66.7 The NHMRC stated that the use or disclosure of health information without consent for the purposes of establishing or maintaining a register is unlikely to comply with the National Privacy Principles (NPPs). Such use and disclosure is unlikely to be a directly related secondary purpose or to be within the reasonable expectations of health consumers. The NHMRC noted that getting consent from all relevant health consumers for their health information to be included in a register is likely to be impracticable and that incomplete data sets substantially impair the utility of such registers.[6]

66.8 The NHMRC noted that establishing such registers would appear to require approval by a Human Research Ethics Committee (HREC), according to the *Guidelines Approved under Section 95A of the Privacy Act 1988*[7] (Section 95A Guidelines), but that it would be difficult for an HREC to decide where the balance of interests lay in relation to an individual register, in the absence of specific information about the proposed future use of the register. The NHMRC noted that health information registers raise significant privacy concerns, but considered that the registers should be permitted within a rigorous ethical and privacy framework that appropriately protects the public interest.[8]

66.9 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the NHMRC gave detailed consideration to the regulation of human genetic research databases, including the issue of consent to future unspecified use of information held in such databases.[9] ALRC 96 made a number of recommendations in this regard, including:

> The National Health and Medical Research Council (NHMRC), as part of its review of the *National Statement on Ethical Conduct in Research Involving Humans* … should amend the National Statement to provide ethical guidance on the establishment, governance and operation of human genetic research databases. The

---

5 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

6 Ibid.

7 National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

8 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004. The Australian Nursing Federation was also of the view that collection of data for health data registers is being impeded by individual organisations' interpretation of the *Privacy Act*: Australian Nursing Federation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 February 2005.

9 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Ch 14.

> amendments (whether by means of a new chapter or otherwise) should include specific guidance on obtaining consent to unspecified future research.[10]

66.10 The revised *National Statement on Ethical Conduct in Human Research* (the National Statement), issued in 2007, includes a new chapter on 'databanks'.[11] The chapter discusses establishing databanks and using the information stored in databanks for research purposes. The National Statement discusses consent requirements for collection of information into databanks, including: 'specific consent' that is limited to a specific research project; 'extended consent' for the use of information in future research projects that are closely related to the original project or in the same general area of research; and 'unspecified consent' for the use of information for any future research. The National Statement includes specific guidance on obtaining such consent and notes the possibility that a researcher may seek permission from an ethical review body to proceed without consent.[12]

66.11 In response to the ALRC's Issues Paper, *Review of Privacy* (IP 31),[13] a number of major research institutions, including the NHMRC and the Australian Institute of Health and Welfare, reiterated that the existing provisions of the *Privacy Act* do not provide an appropriate regime for the establishment, maintenance and use of health registers. In its submission to IP 31, the OPC acknowledged that seeking approval to establish a health register through the HREC mechanism may present difficulties.

> In the absence of a clearly identified purpose, HRECs would be unable to assess where the public interest lay in relation to the register. It may be difficult for researchers to clearly identify all prospective uses of that data at the time of submitting a research proposal. As the NHMRC put it in their submission to the OPC review, 'by the time the questions are obvious, the opportunity to identify the person to whom the information relates or to gain consent to use the health information may be lost'.[14]

Discussion Paper proposals

66.12 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC noted that establishing a health information database or register for research purposes, where the information is to be collected, used or disclosed without consent, would be possible under the proposed research exceptions to the Unified Privacy Principles (UPPs), but would require the approval of an HREC and would have to be done in accordance with the Research Rules issued by the Privacy Commissioner.

---

10 Ibid, Rec 18–1.

11 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), Ch 3.2.

12 Ibid, [2.2.14].

13 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).

14 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

66.13 The ALRC proposed in DP 72 that, to assist HRECs to review proposals to establish health information databases or registers, the following issues should be addressed in the Research Rules to be issued by the Privacy Commissioner:

- the process by which an HREC should review a proposal to establish a health information database or register for research purposes;

- the matters an HREC should take into account in considering whether the public interest in establishing the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and

- the fact that, where a database or register is established on the basis of HREC approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review.[15]

Submissions and consultations

66.14 The OPC expressed qualified support for this proposal noting, however, that the OPC remained of the view that the Privacy Commissioner should not be the party responsible for issuing the Research Rules and that the public interest test should not be amended from 'substantially outweighs' to 'outweighs'. The OPC also reiterated its view that, where a database or register is to be established for broad purposes—for example, to inform the development of public health policy—it should be established by legislation. Enabling legislation would bring the database within the 'required or authorised by law' exceptions to the UPPs and ensure 'the certainty, parliamentary oversight and scrutiny needed to maintain public confidence in the way health and other sensitive information is used'.[16]

66.15 The Department of Health and Ageing (DOHA) was also of the view that, where collection of personal information into a research database was to be mandatory and done without consent, the database should be established by specific legislative provisions.[17]

66.16 The Western Australian Department of Health noted that:

> Guidelines are needed to assist HRECs with the application of the public interest test to research infrastructure projects such as long term data bases or biobanks. In these cases the benefits of the research cannot be effectively evaluated because particular research projects are prospective and have not yet been developed. The value of the

15 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–11.
16 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
17 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

> research is therefore speculative. Factors relevant to evaluating the public interest in these applications should include the administrative procedures for managing and securing the data over the life of the data bank or biobank, the provision of information to participants, the criteria for access and the procedures for protecting privacy.[18]

66.17 A number of stakeholders expressed support for the ALRC's proposal to provide guidance for HRECs in relation to the establishment of registers and databases in the Research Rules to be issued by the Privacy Commissioner.[19] The NHMRC noted that it would be pleased to assist the Privacy Commissioner in developing the rules around the establishment of databases and registers.[20]

ALRC's view

66.18 In Chapter 63, the ALRC recommends that the new *Privacy (Health Information) Regulations* make express provision for the collection, use and disclosure of health information without consent where necessary for the funding, management, planning, monitoring, or evaluation of a health service where:

- the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual;
- it is unreasonable or impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and
- the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.[21]

66.19 A provision along these lines would allow the establishment of health information databases and registers in the health services context where it is necessary to collect identified information and it is unreasonable or impracticable to seek consent. Establishing a database under this provision would not require approval by an HREC, although it would have to be done in accordance with rules issued by the Privacy Commissioner. Personal information held in such databases might then be used for research, but any proposed use would have to be conducted in accordance with the research exceptions to the UPPs and would be subject to HREC approval.

---

18 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

19 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

20 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

21 Rec 63–7.

66.20 The ALRC notes that it will continue to be possible to establish particular databases or registers in the health services context or the research context by legislation, as has been done in the case of the New South Wales Pap Test Register[22] and the National Human Papillomavirus Vaccination Program Register.[23] It will also continue to be possible to establish databases or registers on the basis of consent, including specific, extended or unspecified consent as set out in the National Statement.

66.21 Where such a database is to be established purely for research purposes and the information is to be collected, used or disclosed without consent, this will also be possible under the recommended research exceptions to the model UPPs, but will require the approval of an HREC and will have to be done in accordance with the Research Rules issued by the Privacy Commissioner. On the basis of the recommendations in Chapter 65, such databases will not be confined to databases established for health and medical research, but may include databases in other areas of human research such as sociology and criminology.[24]

66.22 The ALRC notes that it is sometimes difficult for HRECs to decide where the balance of interests lies in relation to an individual register, in the absence of specific information about the proposed future use of the register. Recommendations 65–8 and 65–9 provide that HRECs consider the public interest in a proposed collection, use or disclosure of personal information without consent where it is 'necessary for research', and be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs. The language used in the recommendations is deliberately broad, referring to the review of activities 'necessary for research', rather than review of specific research proposals in order to allow the review of activities preliminary to research—such as the establishment of registers or sample acquisition, discussed below.

66.23 In addition, Recommendation 65–3 suggests that the definition of research be amended to include the 'compilation and analysis of statistics'. The establishment of a database or register for research purposes might also be characterised as the 'compilation of statistics' and reviewed on that basis.

66.24 Such databases or registers should not be established in the research context, however, in the absence of legislation or ethical review. Both these mechanisms provide a degree of scrutiny and an opportunity to assess the competing public interests. This is appropriate where personal information, including sensitive information such as health information, is to be collected, used and disclosed without consent by researchers. Agencies or organisations proposing to establish databases or

---

22 *Public Health Act 1991* (NSW) pt 3B.
23 *National Health Amendment (National HPV Vaccination Program Register) Act 2007* (Cth).
24 Rec 65–2.

registers for research purposes should be able to describe the potential future uses and benefits of the database at some level and to provide an HREC with enough information to allow the HREC to consider whether the public interest in establishing the database outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*. If the public interest in establishing the database cannot be demonstrated, the UPPs should prevail. In these circumstances it may be more appropriate to proceed on the basis of consent.

66.25 The ALRC notes that it would also be possible to seek a public interest determination from the Privacy Commissioner allowing the establishment of databases or registers for research. This process would also provide scrutiny and the opportunity to weigh the competing public interests.

66.26 In DP 72, the ALRC proposed that the Research Rules to be issued by the Privacy Commissioner under the research exceptions to the UPPs should address the process by which an HREC might review a proposal to establish a database or register for research purposes, as well as the matters an HREC should take into account in considering the public interest balance. The ALRC has considered this matter further, and is of the view that the Research Rules should be addressed to agencies and organisations that wish to establish a database or register, rather than HRECs. The Research Rules are intended to regulate the collection, use and disclosure of personal information by agencies and organisations for research purposes, rather than the conduct of HRECs.

66.27 The ALRC recommends, therefore, that the rules to be issued by the Privacy Commissioner should address in what circumstances and under what conditions it is appropriate to collect, use or disclose personal information without consent for inclusion in a database or register for research purposes. This will assist HRECs in their deliberations by setting out an acceptable framework for the establishment of databases and registers in the research context. The Privacy Commissioner and the authors of the National Statement may wish to consider providing HRECs with further assistance in the form of guidelines discussing the matters an HREC should take into account in considering the public interest balance. Such guidelines should not, however, be included in the Research Rules themselves.

66.28 The rules should make clear that where a database or register is established without consent on the basis of HREC approval, that approval does not extend to future unspecified uses. Any future use of the database or register for research would require separate consideration.

Recommendation 66–1 The Privacy Commissioner should address the following matters in the Research Rules:

(a) in what circumstances and under what conditions it is appropriate to collect, use or disclose personal information without consent for inclusion in a database or register for research purposes; and

(b) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

Using and linking information in databases

Background

66.29 Databases of health information provide the opportunity to link data more effectively. Dr Roger Magnusson notes that:

> Future improvements in public health will increasingly depend on the more effective use of health data resources in order: to monitor trends in health status, to investigate the causal roles of 'lifestyle', environmental and other risk factors … to measure and improve the quality and performance of health care services and to develop 'best practice' for prevention and care. Epidemiologists and population health researchers, in particular, are keen to unlock the public health value of clinical data …
>
> Identifying and investigating the relationships between risk factors and disease frequently requires researchers to accurately match longitudinal data relating to the same individual.[25]

66.30 The National Health Information Management Group Guidelines note that:

> Most [health registers] will be intended to facilitate further research, for example, through record linkage to other data sets or establishing a sample frame for a more detailed study of a health problem or for clinical trials.[26]

66.31 The National Collaborative Research Infrastructure Strategy (NCRIS) is an Australian Government program announced in 2004 with funding of $542 million to 'provide researchers with major research facilities, supporting infrastructure and

25 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 8–11.

26 Australian Institute of Health and Welfare, *Minimum Guidelines for Health Registers for Statistical and Research Purposes* (2001), 2.

networks necessary for world-class research'.[27] One major focus of the Strategy is population health and clinical data linkage:

> Australia is an international leader in the scope and extent of health-related data collected at the population level. With new technologies, the potential exists to integrate and link data sets, providing a valuable new resource for monitoring the health of the population and the effectiveness of health services, and for research.
>
> The NCRIS *Population health and clinical data linkage* capability aims: to enhance the linkage and integration of health-related data collected in Australia; to provide improved accessibility to these data for the research sector; and to support the development of improved data collection systems.[28]

66.32 The *Privacy Act*, like the National Statement, recognises that in some circumstances it is very difficult or impossible to conduct this kind of research in a way that complies with the Information Privacy Principles (IPPs) and NPPs. As discussed in Chapter 64, the *Privacy Act* provides a mechanism to allow such research to go forward on the basis of approval by an HREC. The National Statement also requires that, where information in a databank is stored in identified or identifiable form, any research proposing to make use of the information be ethically reviewed.

66.33 One stakeholder noted that the process of linking health information for research could be distinguished from the linking of health information for clinical purposes. Those delivering clinical care need to know the identity of the individual and to have access to that individual's health information. Researchers generally do not need to know the identity of the individual, simply that certain health information relates to the same individual. This can be achieved through processes whereby independent intermediaries perform the linking of information, but do not have access to actual health information and researchers have access to the linked health information but not the identity of the individual.[29]

66.34 In ALRC 96, the ALRC and AHEC considered the use of independent intermediaries to hold codes linking genetic samples or information with identifiers. The ALRC and AHEC concluded that use of an independent intermediary (such as a 'gene trustee') is an effective method of protecting the privacy of samples and information held in human genetic research databases. The system maintains the privacy of samples and information, while allowing donors to be contacted if necessary. It ensures that anyone who obtains access to samples and information is unable to re-identify them without the authorisation of the gene trustee.[30] The ALRC and AHEC recommended that:

---

27 Australian Government Department of Education, Science and Training, *National Collaborative Research Infrastructure Strategy* <www.ncris.dest.gov.au/> at 1 August 2007.

28 Ibid.

29 A Smith, *Submission PR 79*, 2 January 2007.

30 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [18.102]–[18.117].

> The NHMRC, in revising the National Statement in accordance with Recommendation 18–1, should provide guidance on the circumstances in which the use of an independent intermediary is to be a condition of: (a) registration of a human genetic research database; or (b) approval by a Human Research Ethics Committee of research involving a human genetic research database.[31]

66.35 The NHMRC has expressed support for these conclusions and noted that they also apply more broadly to non-genetic research databases.[32]

66.36 In its submission, the CSIRO discussed the development of the Data Linkage Unit (DLU) in Western Australia and the New South Wales/ACT Centre for Health Record Linkage, and noted that such units are likely to increase through the NCRIS Population Health and Clinical Data Linkage program.[33]

66.37 The DLU is a co-operative scheme between the Information Collection and Management Branch at the Western Australian Department of Health, the Centre for Health Services Research at the University of Western Australia, the Division of Health Sciences at Curtin University of Technology, and the Telethon Institute for Child Health Research. The DLU was established in 1995 to develop and maintain a system of linkages connecting health information about individuals in Western Australia. The DLU's website states that:

> These linkages are created and maintained using rigorous internationally accepted privacy-sensitive protocols, probabilistic matching and extensive clerical review. The core Data Linkage System consists of links within and between the State's seven core population health datasets, spanning 35 years. This is augmented through links to an extensive collection of external research and clinical datasets. Data can be requested for ethically approved research, planning and evaluation projects, which aim to improve the health of Western Australians.[34]

66.38 In its submission, the Western Australian Department of Health noted that the

> DLU uses a two stage data linkage protocol that allows linkage infrastructure (or linkage keys) to be created using identifying information. Linkable datasets containing encrypted identifiers can then be provided to researchers by data custodians with minimal risk of re-identification or unauthorized linkage to another data source. The linkage infrastructure is updated and managed separately from any clinical or service information. The DLU acts as an intermediary similar to a 'gene trustee'. Ethics clearance is required for the creation of new linkages and use of the linkage infrastructure.[35]

---

31 Ibid, Rec 18–3.

32 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

33 CSIRO, *Submission PR 176*, 6 February 2007.

34 University of Western Australia—School of Population Health, *WA Data Linkage Unit* <www.populationhealth.uwa.edu.au/welcome/research/dlu/linkage> at 1 August 2007.

35 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

66.39 The DLU has now entered into an arrangement with the Australian Government to allow access to Australian Government held aged care information as well as information in the Medicare Benefits Scheme and the Pharmaceutical Benefits Scheme databases. The Western Australian Department of Health and DOHA have entered into a Memorandum of Understanding (MOU) formalising the arrangements and a 'best practice protocol' has been developed to address privacy concerns and other issues.[36]

66.40 In its submission,[37] however, the OPC expressed the view that the method employed by the DLU would not be consistent with NPP 10.4, which provides:

> If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

66.41 The OPC's view is based on the requirement that the information is 'permanently de-identified'. The maintenance of the linkage infrastructure means that information is not permanently de-identified even though an organisation takes reasonable steps to ensure that the information is not disclosed in a form that would identify individuals or from which individuals could be reasonably identifiable. The linkage infrastructure can technically be used to re-identify the information, although this could be done only with the cooperation of the DLU. In ALRC 96, the ALRC and AHEC concluded that maintaining the linkage infrastructure can be important in order to allow individuals to be contacted if research produces information that is of importance to their future health.[38]

66.42 Recommendation 65–9, which sets out the wording for the research exception to the 'Use and Disclosure' principle includes a suggested amendment to the wording of NPP 10.4, so that the provision no longer requires that reasonable steps be taken 'to permanently de-identify' information before it is disclosed. In the ALRC's view, it is sufficient to require agencies and organisations that collect sensitive information under the research exception to take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

66.43 An amendment of this kind would allow researchers to access information through independent intermediaries without requiring the destruction of the linkage infrastructure. If appropriate arrangements are put in place—for example, intermediaries are sufficiently independent and data recipients only receive information that does not identify individuals—in the ALRC's view, the information held by the data recipient will be adequately protected for the purposes of the *Privacy Act*.

---

36 University of Western Australia—School of Population Health, *WA Data Linkage Unit* <www.populationhealth.uwa.edu.au/welcome/research/dlu/linkage> at 1 August 2007.

37 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

38 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Ch 16.

66.44 The Centre for Health Record Linkage is a co-operative scheme established by NSW Health, the Cancer Institute NSW, the Clinical Excellence Commission, the University of Sydney, the University of New South Wales, the University of Newcastle, ACT Health and The Sax Institute. The Centre, like the DLU, creates master linkage keys allowing researchers to link information about particular individuals in different databases in New South Wales and the ACT without being able to identify the individuals.

66.45 In its submission, the CSIRO discussed another data-linkage model that offered researchers access to information within a privacy protective environment:

> In recognition of the widespread challenge of generating information from databases which include personal information and at the same time not compromising standards of privacy and confidentiality, CSIRO has been developing new privacy-enhancing technologies, including:
>
> - Health Data Integration™ (HDI™)—software which enables linking of patient records from different data repositories without requiring identifying information to be revealed to any other party. Any external release of the data through HDI™ is controlled by the data custodian, and can be stopped at any time.
>
> - Privacy-Preserving Analytics™ (PPA™)—software developed for analysing confidential data without compromising confidentiality. The PPA techniques allow analysis of confidential raw data, but filter the outputs delivered to the researcher in order to protect the privacy of individuals and organisations and to respect data custodians' responsibilities not to release confidential information.[39]

66.46 There are other models being used around Australia such as the Bio21: Molecular Medicine Informatics Model (MMIM) currently being piloted in Victoria, which aims to allow authorised researchers to conduct research 'confident that ethics, privacy, security and IP issues are addressed'. The Bio21: MMIM website states that the model will provide

> clinical research collaborators from universities, research institutes and teaching hospitals with ethical approval [with] access [to] secure, privacy protected research information, that spans multiple disease groups and multiple organisations.[40]

66.47 The Department of Human Services suggested that:

> There is little guidance in the *Privacy Act* for these issues, which leads to differing interpretations being made by organisations dealing with health registers. A set of minimum standards should be developed to facilitate effective/safe linkage processes to allow important research to be conducted, without identifying particular individuals where no consent has been obtained. Medicare Australia believes the example

39 CSIRO, *Submission PR 176*, 6 February 2007.

40 Melbourne Health, *Molecular Medicine Informatics Model* (2007) <mmim.ssg.org.au/> at 1 August 2007.

> presented by the Cross-Jurisdictional Linkage of Administrative Health Data project, underpinned by an MoU between DoHA and WA Department of Health, could be a good model on which to base the set of minimum standards.[41]

66.48 In its submission to the OPC Review, the NHMRC noted that some HRECs appear to reject research proposals automatically where they involve data linkage of health information without consent, apparently in the 'mistaken belief that such linkage is not ethically or legally acceptable'.[42] The revised National Statement makes clear that approval may be given to use such data even in the absence of consent, for example, where the research involves linkage of data sets and the use of identifiable data is necessary to ensure that the linkage is accurate.[43]

66.49 A number of other issues were raised in response to IP 31. The NHMRC highlighted a particular problem for researchers in gaining access to data registers in order to identify health consumers with specific characteristics relevant to a research proposal. This activity, described as 'sample acquisition', may pre-date the development of a formal research proposal and, in the NHMRC's view, is unlikely to be consistent with the IPPs or NPPs. The NHMRC considered, however, that sample acquisition was important and should be facilitated by the *Privacy Act*.[44]

66.50 In relation to sample acquisition the OPC noted that the research exceptions in NPPs 2 and 10 cover activities *necessary* for research, and expressed the view that sample acquisition was such an activity and would be covered by the exceptions. The OPC noted, however, that sample acquisition might not be covered by the 'conduct of medical research' exception to the IPPs.[45]

Discussion Paper proposals

66.51 In DP 72, the ALRC expressed the view that 'sample acquisition' is an activity necessary for research and should be supported by the provisions of the *Privacy Act.* The ALRC noted the OPC's advice that this activity is allowed under the existing provisions of NPPs 2 and 10. The ALRC proposed that the Research Rules should address the process by which an HREC might review a sample acquisition proposal, as well as the matters an HREC should take into account in considering the public interest balance involved in allowing access to databases and registers for research purposes.[46]

---

41 Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

42 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

43 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [3.2.4].

44 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

45 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

46 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–12.

66.52 The ALRC also proposed that agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes, should consult the OPC to ensure that such systems or infrastructure met the requirements of the *Privacy Act*.[47]

Submissions and consultations

66.53 A number of stakeholders expressed support for the proposal to address sample acquisition and the public interest balance around the use of databases and registers for research in the Research Rules.[48] The OPC also expressed support for these issues to be dealt with in the rules, while maintaining its position that the rules should not be issued by the Privacy Commissioner and the public interest test should not be changed.[49]

66.54 A number of stakeholders expressed support for the proposal to consult with the OPC to ensure that research systems and infrastructure met the requirements of the *Privacy Act*.[50] The OPC noted that, while providing advice and guidance on the Act was one of the functions of the Privacy Commissioner, the Office was unlikely to be able to respond in detail to all such requests for advice. The OPC encouraged agencies and organisations to conduct privacy impact assessments (PIAs) in relation to projects—such as the establishment of research systems and infrastructure—that may have a significant impact on privacy.[51]

66.55 In its submission, the Alfred Hospital Ethics Committee stated that, in considering the public interest in the use of health information databases, HRECs should be required to consider:

- the importance of the research question;
- the imposition on privacy;
- the security of data;

---

47 Ibid, Proposal 58–13.

48 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Western Sydney Human Research Ethics Committee, *Submission PR 418*, 7 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

49 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

50 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007.

51 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

- the seniority/quality of the researchers;
- the consequences of requiring that consent be obtained; and
- the consequences of inappropriate use or disclosure.[52]

ALRC's view

66.56 There are a number of different models being adopted around Australia to allow researchers to have access to and to link personal information in ways that do not identify individuals. The ALRC has not formed a view that one model should be preferred over another. It is possible that each of the various models provides sufficient protection to comply with the *Privacy Act*. That will depend, however, on the details of the various models, their technical specifications and their governance arrangements.

66.57 Some high-level guidance on these issues may be included in the Research Rules, to be issued by the Privacy Commissioner, but in the final analysis, whether a particular model meets the requirements of the *Privacy Act* will have to be decided on a case-by-case basis. It is the responsibility of agencies and organisations to ensure that such schemes comply with the Act.

66.58 The ALRC agrees with the OPC that agencies and organisations should be encouraged to conduct PIAs for new projects and developments that may have a significant impact on the handling of personal information, including the establishment of systems or infrastructure to allow the linkage of personal information for research purposes.[53]

66.59 In DP 72, the ALRC proposed that the Research Rules should address the process by which an HREC might review a proposal to examine a database or register to identify potential participants in research, and the matters an HREC should take into account in considering the public interest balance around this activity. The ALRC has considered this matter further, and is of the view that the Research Rules should be addressed to agencies and organisations that wish to collect, use or disclose information in a database or register, rather than HRECs. The rules to be issued under the research exceptions are intended to regulate the collection, use and disclosure of personal information by agencies and organisations for research purposes, rather than the conduct of HRECs.

66.60 The ALRC recommends, therefore, that the Research Rules, to be issued by the Privacy Commissioner, should address in what circumstances and under what conditions it is appropriate to collect, use or disclose personal information without consent in order to identify potential participants in research. The content of these rules

---

52 General Ethical Issues Sub-Committee—Alfred Hospital Ethics Committee, *Submission PR 531*, 21 December 2007.

53 PIAs are discussed in detail in Ch 47.

will assist HRECs in their deliberations by setting out an acceptable framework for the use of databases and registers for 'sample acquisition' in the research context. The Privacy Commissioner and the authors of the National Statement may wish to consider providing HRECs with further assistance in the form of guidelines discussing the matters an HREC should take into account in considering the public interest balance but these guidelines should not be included in the Research Rules themselves.

Recommendation 66–2 Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should conduct a Privacy Impact Assessment to ensure that the privacy risks involved are assessed and adequately managed in the design and implementation of the project.

Recommendation 66–3 The Research Rules, to be issued by the Privacy Commissioner, should address the circumstances in which, and the conditions under which, it is appropriate to collect, use or disclose personal information without consent in order to identify potential participants in research.

Part I

Children, Young People and Adults Requiring Assistance

67. Children, Young People and Attitudes to Privacy

Contents

Introduction

67.1 This chapter examines whether children and young people have different attitudes to privacy from older people.[1] It commences by discussing existing Australian and overseas research about attitudes of children and young people to privacy. It then sets out the methods the ALRC used to consult with children and young people in this Inquiry, and highlights some of the privacy-related issues that were said to be of

1 In this Report, the term 'child' is used to mean an individual under the age of 13.

concern to these children and young people. Finally, it considers the privacy of children and young people who participate in online social networking.

67.2 In this chapter, the ALRC recommends that a longitudinal study of the privacy attitudes of Australians, and in particular attitudes of young Australians, be undertaken to underpin future policy making in this area. The ALRC does not make any recommendations for regulation of social networking websites additional to the requirements of the *Privacy Act*. It does, however, make a number of recommendations aimed at increasing the levels of awareness of privacy issues among children and young people.

67.3 Chapter 68 deals specifically with issues about individuals under the age of 18 making decisions in relation to the *Privacy Act 1988* (Cth), and Chapter 69 deals with a number of particular privacy issues relevant to children and young people.

Generational differences in attitudes to privacy

67.4 Traditionally, a generation was defined as the average interval of time between the birth of a parent and the birth of his or her offspring. Social researchers today, however, define a generation as a cohort of people born into and shaped by a particular span of time. For example, McCrindle Research has analysed Australian Bureau of Statistics data of birth rate rises and declines in order to delineate distinct generational groups. The social changes and trends affecting these groups provide context for their generational definitions.

67.5 Generational definitions are generalisations. There always will be individuals who do not fit the stereotype of a particular generation. Generational definitions, however, may help to reveal the key social drivers and expectations of different sections of the population.

67.6 In recent years, there has been much discussion about the attributes and attitudes of members of 'Generation Y'—namely, the generation of people born between 1980 and 1994. Research into Generation Y does not tend to focus on privacy-related issues. Nevertheless, it helps to clarify how members of this generation conceptualise privacy by describing their experiences, needs and ambitions more generally.

Table 67.1: Australia's Generations[2]

Description	Born	Age	Pop'n	(% of Pop'n)
Builders	Before 1946	63+	3.5m	17%
Boomers	1946–1964	44–62	5.3m	26%
Generation X	1965–1979	29–43	4.4m	21.5%
Generation Y	1980–1994	14–28	4.2m	20.5%
Generation Z	1995–2009	Under 14	3.1m	15%

67.7 The members of Generation Y are said to share a number of key characteristics.

- They are completely adept at using communications technologies, such as the internet, email, instant messaging and mobile technologies. They have grown up wit these technologies and their social worlds and expectations are completely integrated with the existence of these technologies because they have never known a world in which they did not exist.

- They have experienced (directly or indirectly) split households and working parents. Accordingly, social networks are of vital importance to them and they keep in touch constantly through the use of communications technologies.

- They live in a global village, where they can communicate with virtually anyone through a variety of instantaneous media, and are considered to belong to the most embracing, non-racist, non-gender biased generation yet.

- They are optimistic and have high expectations, along with the confidence that they will realise these expectations. This can be compared to members of Generation X, who are said to be apathetic and pessimistic.

- Due to their self confidence they are considered fickle and demanding, and willing to move quickly to take up new opportunities.[3]

---

2 Table 67.1 is based on a similar table in McCrindle Research, *New Generations at Work: Attracting, Recruiting & Training Generation Y* (2006), 8. In the United States, the Builders are often referred to as the 'Silent Generation'.

3 See, eg, Ibid; R Huntley, *The World According to Y: Inside the New Adult Generation* (2006); N Howe and W Strauss, *Millennials Rising: The Next Great Generation* (2000).

67.8 It is often argued that the behaviour of young people can be attributed to youth rather than generational attitudes. If this were the case, however, young people today would be indistinguishable from young people a generation ago.[4] Currently, it could be argued that the dependence of members of Generation Y on social networks of friends is an attribute of youth as opposed to an attribute of a generation. Members of Generation Y, however, are said to be retaining their dependence on social networks of friends as they enter adulthood and are said to believe that their friends will remain friends for life.[5]

67.9 Australian social researcher Hugh Mackay studied the attitudes of 19 year olds in 1980 and in 2000.[6] His research revealed that attitudes among this demographic have moved from pessimism to optimism over this period of time. Nineteen year olds in 1980 were pre-occupied with the state of the world, the threat of nuclear annihilation, widespread terrorist activity, growing economic dislocation and recurring industrial trouble. In contrast, 19 year olds in 2000 were utterly confident about their own, and the world's, long-term survival. Dr Rebecca Huntley suggests that, even after the events of 11 September 2001, the 2002 Bali bombings and the 2006 London bombings, today's young adults have a sense of optimism and confidence, and are either more capable of facing the world's problems or more effective at ignoring them.[7]

> In Australia, Generation Y's anger around [September] 11 was less about the event itself than the reaction of the United States government and its allies. Many young adults have reacted negatively to the media hype around the tragedy and the relentless and insensitive use of images of death and destruction to sell papers and increase TV ratings. And whilst this was Generation Y's first exposure to international terrorism on a grand scale, most Yers were aware that in so many other places around the world this kind of stuff happens all the time. For many of them now, September 11 intensified their desire to enjoy life right now.[8]

67.10 While commentators can make generalisations about the attitudes of Generation Y, it remains unknown whether these attitudes are widespread and will remain with these young people as they progress through life.

Attitudes of young people to privacy

Australian research

67.11 There is limited Australian research on the attitudes of young people to privacy. An online survey regarding Australian privacy legislation was conducted in 2007 by the United Nations Youth Association in South Australia, Flinders Law Students'

---

4 McCrindle Research, *New Generations at Work: Attracting, Recruiting & Training Generation Y* (2006), 13.

5 N Howe and W Strauss, *Millennials Rising: The Next Great Generation* (2000), 214–219.

6 H Mackay, *The Mackay Report: Leaving School* (2000), 26.

7 R Huntley, *The World According to Y: Inside the New Adult Generation* (2006), 9.

8 Ibid, 4.

Association and the Adelaide University Law Students' Society.[9] Of the 332 respondents, 21.9% were aged 26 or over, 67.6% were aged 18–25, 9.6% were aged 15–17, and 0.6% (2 respondents) were under the age of 15. The vast majority of respondents were resident in South Australia, with 73% living in Adelaide.

67.12 This survey provides a snapshot of the attitudes of young people to privacy, particularly those of tertiary students in South Australia. The survey revealed that:

- 95.5% of respondents considered privacy to be a human right, and 92.5% described it as being important or very important;
- the handling of personal information by businesses and other individuals caused respondents the most concern. The handling of personal information by government departments and intelligence organisations caused respondents less concern, and the handling of personal information by medical and health service providers caused respondents the least concern;
- 77.6% of respondents were of the view that technology imposes a significant or strong threat to privacy, and 40.6% indicated that photographs or video footage of them had been posted on the internet without their permission;
- while some 220 respondents indicated they thought their privacy had been infringed at some point in time, only four had made a formal complaint to a privacy commissioner or ombudsman;
- 59.5% of respondents suggested that at 16–17 years of age most young people have the capacity to make decisions about their personal information; 22.2% indicated this occurred at 14–15 years of age, and 2.7% indicated that it occurred at 12–13 years of age; and
- while 16.8% of respondents indicated that young people under the age of 18 should not be able to seek medical treatment without the knowledge and consent of their parents or guardians, most of the respondents in this category were over the age of 25.

67.13 A number of general surveys on attitudes to privacy provide additional information on how the 18–24 age group perceive privacy.

---

9 The survey methodology and results were provided to the ALRC as a submission to this Inquiry: United Nations Youth Association, Flinders University Students' Association and Adelaide University Law Students' Society, *Submission PR 557,* 7 January 2007. The results have not as yet been published elsewhere.

67.14 The Office of the Privacy Commissioner (OPC) has conducted four surveys of community attitudes to privacy.[10] The surveys were quantitative in nature and involved telephone interviews with respondents representative of the adult population nationwide.[11] The 2001, 2004 and 2007 surveys separate data by age groups.[12] Some of the key points from the 2007 survey are set out below.

- Young people aged 18–24 are less likely than the rest of the adult population to be aware of the existence of federal privacy laws—the percentage of this age group that are aware of federal privacy laws in 2007 (50%) remained about the same as the 2004 figure of 48%, while the average figure for the whole adult population rose from 60% in 2004 to 69% in 2007.[13]

- Young people are less likely than the rest of the adult population to be aware of the existence of the federal Privacy Commissioner.[14]

- Awareness of the existence of the federal Privacy Commissioner increases with age.[15]

- Concern about providing others with personal financial information increased with age.[16]

- Younger Australians are most concerned about providing others with their home telephone number or home address.[17]

- Young people are much more likely to provide personal information in order to receive a discount or to win a prize. The percentages of people willing to provide personal information for these purposes dropped steadily through the age groups. For example, 39% of those aged 18–24 indicated that they would provide personal information to obtain a discount (as opposed to 54% in 2004). Only 15% of those aged 50 and over indicated that they would provide personal information for this purpose.[18]

---

10 Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007); Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004); Roy Morgan Research, *Privacy and the Community [prepared for Office of the Federal Privacy Commissioner]* (2001). A similar survey was conducted by Roy Morgan Research in 1999.

11 While Roy Morgan Research undertook some qualitative research as part of the 2001 survey, there was no report on the outcome of that research.

12 The 2007 survey deliberately over-sampled the 18–24 age group to ensure that the responses of younger Australians could be compared to those aged 25 and over: Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), 3.

13 Ibid, 6.

14 Ibid, 8.

15 Ibid, 8.

16 Ibid, 24.

17 Ibid, 24.

18 Ibid, 31–32.

- There are no significant differences in the attitudes of members of different age groups to the question of whether the inclusion of health records on a database should be voluntary. This differs from the position in 2004 when younger people were more likely than people in older age groups to consider that inclusion should be voluntary. The overall percentage supporting voluntary inclusion was 76% in 2007, up from 64% in 2004.[19]

- Young people are much more likely to have provided false information when completing online forms in order to protect their privacy, with 58% of those aged 18–24 admitting to this practice, in comparison to only 8% of those aged 50 and over.[20]

67.15 A 2005 survey of the use of the internet and some other forms of technology by Australian children and young people is also of interest.[21] The survey found that, while Australian children are not using the internet as frequently as children in Hong Kong or the United Kingdom, the frequency of use has increased. Thirty seven per cent of Australian children with a home internet connection log on daily, and a further 34% log on at least two or three times a week. The survey also showed that frequency of use increased with age; and that girls and older children were more likely to use the internet as a communication resource (for email and instant messaging) than boys and younger children, who were more focused on access for entertainment purposes (games, websites, music).

67.16 This survey indicates that large numbers of Australian children and young people are making regular use of online technology, in some cases with limited or no supervision. This proposition is supported by a more recent 2006 survey by the Australian Bureau of Statistics of children's participation in cultural and leisure activities. This survey reveals that 65% of children aged 5–14 years use the internet, with 73% of these children using it more than once a week.[22]

Overseas research

67.17 In 2005, the Hong Kong Federation of Youth Groups and the Hong Kong Office of the Privacy Commissioner for Personal Data conducted a survey of the attitudes of people aged 15–29 to privacy.[23] Although it was a limited survey, with a particular emphasis on online transactions, the results indicate that young people in Hong Kong

---

19 Ibid, 45.
20 Ibid, 64.
21 Netratings Australia Pty Ltd, *kidsonline@home: Internet Use in Australian Homes [prepared for Australian Broadcasting Authority and NetAlert Limited]* (2005).
22 Australian Bureau of Statistics, *Children's Participation in Cultural and Leisure Activities, Australia, Apr 2006*, 4901.0 (2006).
23 Hong Kong Federation of Youth Groups, *2005 Survey of Youth Attitudes and Perceptions Towards Personal Data Privacy* (2005).

appear to have similar attitudes to privacy as young people in Australia—that is, they have concerns about certain privacy issues, but also consider certain types of initiatives, such as a patient medical records databases, to be worthwhile.

67.18 Of particular interest in the survey were two questions regarding the taking of photographs by strangers. Fourteen per cent of respondents admitted to having taken a photograph of a stranger without first asking permission; and 21% disagreed or strongly disagreed with the suggestion that taking a photograph of a person in a public place without permission is an invasion of personal data privacy rights.[24] There was no age breakdown of responses to these questions to see if responses differed according to the ages of the respondents

67.19 In October 2007, research conducted for the United Kingdom Information Commissioner's Office on privacy issues in the online environment was completed. The research examined the online activities of 2,000 United Kingdom internet users aged 14–21.[25] The research revealed that:

- 60% of respondents had posted their date of birth, and 59% had posted their personal email address, on a social networking website, chatroom or blog. Boys appeared to be slightly more cautious than girls about posting personal information. Older respondents were less cautious than those aged 14–17;

- 52% of respondents indicated that they considered privacy to be important, but that they liked to meet new people so tended to leave some of their profile public. Only 7% indicated that privacy was not important at all and that they left their profile completely open;

- 58% of respondents indicated they had never thought that what they put online now might still be there in five, 10 or 20 years time; and

- 52% indicated they usually skim read and possess a rough understanding of website privacy policies, while 32% indicated they had never read an online privacy policy and 2% indicated they did not know what a privacy policy was.

67.20 A study in the United States of 'the lives of young Americans as they make the transition to adulthood' also addressed the privacy of young people.[26] In April 2006, 1021 adults aged 18–24 were surveyed for the study. Respondents to the survey generally valued privacy, but considered it to be of equal value to the ease and

---

24 Ibid, 2.

25 Dubit Research, *Data Protection—Topline Report [commissioned by United Kingdom Information Commissioner's Office]* (2007).

26 Greenburg Quinlan Rosner and Polimetrix, *Youth Monitor: Coming of Age in America* (2005), 1. See in particular *Part IV—The MySpace Generation* (2006).

convenience presented by the internet.[27] Seventy-eight per cent indicated that they had a personal website, webpage or blog and regularly participated in online communities such as MySpace or Facebook. Those who did not belong to online communities were more likely to place a higher value on privacy than convenience.

67.21 The research suggests that members of Generation Y balance their concern about privacy and their desire for convenience by self-censoring the types of personal information they make available online. Nevertheless, members of older generations may be shocked at the level of detail and the types of information young people feel comfortable about sharing. For example, 16% post their home address and 78% post photographs (often unflattering or 'sexy' photographs) online. Young people in the online environment appear to be more concerned about identity theft and receiving spam than they are about stalking and harassment (although the latter worries their parents).

67.22 In 2006, a more focused survey of teenagers aged 12–17, and their parents, was conducted in the United States to examine how teenagers manage their online identities and personal information when using online social networks.[28] Some of the key findings of this survey were that:

- 93% of American teenagers use the internet (an increase from 87% in 2004), and 55% of them have online profiles;
- 66% of the teenagers with online profiles limit access to the profile in some way;
- 82% of teenagers with online profiles include their first name in the profile, and 79% include photographs of themselves. Varying percentages include information such as the name of their city or town (61%); the name of their school (49%); their email address (29%); their last name (29%); and their mobile phone number (2%);
- Boys are more likely than girls to post false information, sometimes for reasons of privacy, but also at times to be playful or silly; and older teens are more likely than younger teens to disclose more personal information;

---

27 Greenburg Quinlan Rosner and Polimetrix, *Youth Monitor: Coming of Age in America Part IV—The MySpace Generation* (2006), 1912.

28 A Lenhart and M Madden, *Teens, Privacy & Online Social Networks* (2007) Pew Internet & American Life Project.

- 41% of teenagers using the internet believe their online activity is monitored by their parents (an increase from 33% in 2004), while 65% of parents reported monitoring their teenager's online activity.

67.23 One of the key questions the survey sought to answer was whether today's teenagers were less concerned about their privacy because the internet gives them so many opportunities to socialise and share information. The researchers found that

> there was a wide range of views among teens about privacy and disclosure of personal information. Whether in an online or offline context, teenagers do not fall neatly into clear-cut groups when it comes to their willingness to disclose information or the way they restrict access to the information that they do share. For most teens, decisions about privacy and disclosure depend on the nature of the encounter and their own personal circumstances. Teen decisions about whether to disclose or not involve questions like these: Do you live in a small town or big city? How did you create your network of online 'friends'? How old are you? Are you male or female? Do your parents have lots of rules about internet use? Do your parents view your profile? All these questions and more inform the decisions that teens make about how they present themselves online. Many, but not all, teens are aware of the risks of putting information online in a public and durable environment. Many, but certainly not all, teens make thoughtful choices about what to share in what context.[29]

67.24 In a United States poll, the government's policy of eavesdropping on suspected terrorists' telephone calls and emails without a warrant was considered wrong by 56% of 18–29 year olds (compared to 53% of 50–64 year olds who said it was the right thing to do).[30] Some of the young people criticising the government surveillance share intimate details in the online environment—an apparent contradiction. The contradiction, however, appears to be explained by young people's attitudes to control of the flow of personal information. According to one young adult, for example, 'what I get concerned about is when that control gets compromised without my consent'.[31]

ALRC consultations with young people

67.25 As noted above, there is limited literature on the attitudes of young people in Australia to privacy. In the early stages of the Inquiry, the ALRC determined that there was a need to assess if young people in Australia possess similar attitudes to those possessed by young people overseas. The usual submission and consultation process undertaken by the ALRC does not preclude the participation of young people. Experience indicates, however, that traditionally young people do not engage in these processes without specific prompting. Accordingly, the ALRC developed a number of processes particularly aimed at young people.

---

29 Ibid, iv.

30 J Berton, 'The Age of Privacy: Gen Y Not Shy Sharing Online—But Worries About Spying', *San Francisco Chronicle* (online), 20 May 2006, <www.sfgate.com>.

31 Ibid.

67.26 An age indicator box was placed on all of the pages that allowed people to submit comments to the Inquiry via the ALRC's website. While optional, this indicator was useful in helping the ALRC to determine whether the views of stakeholders differed according to their age.

Talking Privacy website

67.27 In early 2007, the ALRC developed a website called 'Talking Privacy', which was accessible from the ALRC's home page. The aim of the Talking Privacy website was to engage young people using a familiar and well-used medium. Designed specifically to appeal to young people, the website contained information about the Privacy Inquiry, links to further information about privacy law, and encouraged young people to send in comments to the ALRC about their privacy issues or experiences.

67.28 Following the release of the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the website was updated to include a description of the ALRC's proposals relating to children and young people. The website also contained information aimed particularly at teachers and students who were considering law reform or privacy as part of a school curriculum.

Youth workshops

67.29 As noted in Chapter 1, the ALRC held a number of public forums during the Inquiry. In addition, in order to ensure that the views of young people were captured as part of the consultation process, the ALRC developed a workshop format specifically for young people aged 13–25. The format provided young people with an opportunity to discuss general issues about privacy, and to provide comments and views on case studies which raised privacy issues in contexts that were relevant to young people.

67.30 The two-hour workshops were first conducted in late 2006 and early 2007, prior to publication of DP 72. A trial youth workshop was conducted in Sydney with a group of Year 10 and 11 students from Dubbo College Senior Campus. Youth workshops were then conducted in Perth, Brisbane and Hobart.[32]

67.31 Following publication of DP 72, two further workshops were held in December 2007 with Year 10 students from Fort Street High School and Cherrybrook Technology High School, both in Sydney.

---

32 The Perth workshop was supported by the Western Australian Office for Children and Youth; the Brisbane workshop was supported by the TC Beirne School of Law, University of Queensland; and the Hobart workshop was supported by the Commissioner for Children, Tasmania.

67.32 The number of participants in each workshop varied from five to 20. In total, 74 young people participated in the workshops. The age of the participants ranged from 14 to mid-20s. The workshops were generally well received by the participants, and were effective in capturing the views of young people on privacy-related issues.

67.33 In summary, the workshops indicated that young people in Australia share similar views and opinions to those reported in the research and literature in this area. Young people are aware of privacy issues and have certain concerns about their privacy. The issues of concern to them, however, may not necessarily coincide with the issues of concern to older Australians. As could be expected, most of the issues of concern centred around their experiences, and focused on issues directly affecting them.

67.34 The privacy of personal space was raised in the workshops in discussions about searches of bags and lockers, privacy within the home, and privacy of meeting places such as religious halls. Issues about public surveillance were rarely raised.

67.35 The types of personal information that young people considered sensitive were the same as those considered sensitive under the *Privacy Act*—namely, information about sexual orientation, health, political views, ethnicity, religion and criminal records.

67.36 Much of the discussion in the workshops focused on the ability of individuals to choose what personal information to disclose, and to whom. Participants were often of the view that disclosure of personal information to a person or body did not entitle that person or body to use the information for a different purpose. This is consistent with the existing privacy principles and the model Unified Privacy Principles. It also is consistent with past consultations conducted by the New South Wales Commission for Children and Young People.[33] The Commission provided the ALRC with a quote from one young person which sums up a typical reaction of a young person to privacy: 'Privacy matters because it is up to me whether or not I share information and who I share it with'.

67.37 At the same time, most young people accepted that there were many situations in which it may be necessary to disclose personal information for a greater public good—including to employers, police and the government. Young people considered, however, that there should be clear limitations on the mandatory disclosure of personal information. There was a range of views about the extent of the limitations.

67.38 The issue that raised the most concern in the workshops was the disclosure of health information to parents and others. Participants demonstrated a sophisticated understanding of the competing issues in this area—that is, the need to provide confidential medical advice to young people; the need to ensure the ongoing safety and

33 NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007.

well being of young people; the interests and responsibilities of parents; and the professional obligations of members of the medical professional. Generally, however, there was a view that any information disclosed to a medical professional by a young person seeking medical advice on his or her own should be confidential—even in circumstances where the medical professional decided that the young person could not consent to the medical treatment in question. There was general agreement that any decision by a medical professional to disclose personal health information to another person, such as a parent or other medical professional, should first be discussed with the young person. Many of the workshop participants considered it appropriate to encourage voluntary parental involvement in the treatment of young people.

67.39 In all of the youth workshops, young people indicated that they expected confidentiality from members of the counselling profession, such as school counsellors. There was strong support for the proposition that information disclosed in counselling sessions should be confidential, except in the limited circumstance where it was necessary to disclose it for the safety and wellbeing of the young person. A number of young people indicated that it was their understanding and experience that school counselling services were not confidential. In workshops held after the release of DP 72, young people supported the proposal that school privacy policies should clarify the extent of the confidentiality of school counselling sessions.[34]

67.40 In the workshops conducted after the release of DP 72, participants were asked to discuss the age at which young people were capable of making independent decisions about privacy-related issues. Most considered that the age would differ according to the context and the individual involved. The majority, however, felt comfortable at setting the age at 16, although they acknowledged that in the medical context it should be 15 to be consistent with rules regarding independent access to a Medicare card.[35] A number of participants noted that parents were responsible for their children until they turned 18 and, as such, were of the view that parents should be entitled to access all information about their children until they were of this age.

67.41 Another prominent issue discussed in the workshops was the posting of photographs online. Many young people had personal experience of this practice, and most had pragmatic responses to the issues raised by it. In general, young people thought that it was good practice to obtain a person's consent before taking his or her photograph and posting it on the internet. They also expressed the view that a photographer working for financial gain also should be required to 'share' some of the financial gains with the person in the photograph. It was accepted, however, that it may be impossible to get the consent of every person in every photograph, particularly in situations where a photograph captures a number of people in a public place. Most

---

34 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 60–7.

35 It should be noted that generally the participants in the youth workshops were well-educated young people with family support.

considered the rules limiting or prohibiting the taking of photographs in certain public spaces, such as swimming pools and swimming carnivals, to be sensible.

67.42 Participants in the workshops accepted that it is often difficult to stop individuals from posting unauthorised photographs online. Some went so far as to say that anyone who poses for a photograph impliedly consents to its publication on the internet. One participant commented that the way to prevent the online publication of your image was to 'cover your face'. This suggestion received a negative reaction from people over the age of 25 with whom the ALRC consulted, and is indicative of the way in which young people are developing different norms around the use of the internet for communication purposes.

67.43 Despite acknowledging the difficulties associated with the permanent removal of website content, most young people considered that an individual should be able to have a photograph removed from a website if he or she did not consent to its posting. This was seen as a suitable remedy to the unauthorised publication of a person's image, and was considered to be more practical than putting laws in place to prevent the initial posting. Participants in the workshops placed a significant amount of trust in the reporting mechanisms available on the major social networking websites, although none indicated that they had any experience using such mechanisms.

67.44 Workshop participants displayed varying levels of understanding of the ramifications of the publication of personal information on the internet. Younger participants were the most likely to have posted personal information online, or to have had their personal information posted online by others. Regardless of this, their understanding of the possible privacy implications of the publication of personal information on the internet was more limited than that of older participants.

67.45 The two workshops held in December 2007 involved students aged 15–16. Participants in these workshops reported a high level of usage of social networking websites and demonstrated a good understanding of how these websites worked. There were, however, stark differences in views about the management of online profiles. While one group was very conscious of the need to protect personal information and use the privacy settings built into the websites, the other rejected the use of privacy settings and suggested that the whole point of social networking was to 'put it all out there'. These attitudes appear to have been driven by peer networks, as participants indicated that these issues were not discussed in school classrooms. In both workshops, however, participants expressed surprise when informed that there are limited legal remedies available to individuals who have suffered a serious breach of privacy in the online environment.

67.46 Other privacy-related issues that tend to concern members of older generations did not concern young people in the workshops. For example, government access to personal information (such as school records to verify compliance with Youth Allowance requirements) was generally considered to be appropriate and fair. In addition, while workshop participants considered the covert collection of personal

information by website operators to send spam annoying, and probably a breach of privacy, they were of the view that it was an everyday occurrence that should be addressed through practical, technology-based solutions as opposed to legal remedies. While some participants were concerned about the reach of recent anti-terrorism legislation, many others considered it appropriate and did not consider their own freedoms had been affected by the legislation.

Submissions and other consultations

67.47 The ALRC also made efforts to meet with representatives of children and young people as part of its general consultation processes. Roundtables were held in Sydney and Melbourne with key representatives of children and young people's interests, with the Sydney roundtable also attended by a number of young people. Meetings were held with each of the children's commissioners in New South Wales, Queensland and Tasmania, and submissions were received from a number of bodies representing young people in Australia. Many of the submissions and consultations focused on decision making by individuals under the age of 18, and are addressed in detail in Chapters 68 and 69.

67.48 One young person submitted that:

> Generation Y may be optimistic, but to say care-free is a stretch. We are concerned that people in authority may abuse our rights in regards to privacy. Concerns about privacy for people in my age bracket is primarily in relation to our developing autonomy from parental control. Thus issues such as medical problems, school issues, social issues, sexual matters, and especially issues involving police, are all privacy issues for Generation Y. I am not overly concerned about the government and privacy, it is more a matter of privacy in relation to my autonomy from my parents, and other authority figures, eg teachers.[36]

67.49 The Youth Affairs Council of Victoria (YACVic) submitted that:

> the issues that impact on the actual level of protection that an individual receives could include a lack of personal or community understanding about young people's rights to privacy, difficulties in accessing complaints mechanisms and the power imbalance between a young person and 'professional' often inherent in a situation in which a young person's personal information is being collected.
>
> YACVic believes that young people's privacy is protected well enough in law, but that a range of other measures can be put in place or initiatives taken in order to ensure young people enjoy the highest level of protection and are not disadvantaged.[37]

---

36 J Boggs, *Submission PR 245*, 8 March 2007.

37 Youth Affairs Council of Victoria Inc, *Submission PR 172*, 5 February 2007.

67.50 It is clear that young people often use technology in a way that affects the privacy of others. For instance, a number of Australian schools have recently clamped down on online posting of inappropriate material, including video footage of fights involving school pupils.[38]

Online social networking

Background

67.51 Until recently, the internet was primarily a source of information. Today, however, it is used by many as a means of communication and has become an important part of social relations.[39]

67.52 Many people now engage in online social networking. Social networking websites enable members to meet people; send messages to each other; share information; and to post information, photographs and videos of themselves for others to view.[40] The explosion in the use of social networking websites is part of a cultural shift in the way in which people interact with others.

67.53 The ALRC did not ask a question about online social networking in Issues Paper 31, *Review of Privacy* (IP 31). This issue has, however, received significant media attention since this Inquiry began. There are now numerous academic papers, media articles and online postings discussing the phenomenon. The increased number of Australian participants using online social networking sites led the ALRC to explore the issue with young people after the release of IP 31. The ALRC has concluded that there are privacy concerns around the practice of online social networking which require further consideration.

Online social networking and young people

67.54 Many young people engage in social networking on the internet. Social networking websites—such as MySpace, Facebook, BeBo and YouTube—provide a forum for young people to promote themselves, and share their thoughts and experiences with like-minded young people around the globe. A growing number of social networking websites are aimed at children as young as 6 or 7.[41]

67.55 It also should be noted, however, that not all online social networking is conducted by young people. In May 2007, MySpace Australia had three million

---

38 E Bellamy, 'Schools Act to Stamp Out Technology Abuse', *The Canberra Times* (Canberra), 8 March 2007, 7.

39 J Wyn and others, *Young People, Wellbeing and Communication Technologies [Prepared for Victorian Health Promotion Foundation]* (2005) Youth Research Centre, University of Melbourne.

40 Office of the Privacy Commissioner, *Your Privacy Rights: FAQs—Social Networking* <www.privacy.gov.au/faqs/ypr/#social_networking> at 14 April 2008.

41 'It's Like MySpace, But With Training Wheels', *Sydney Morning Herald* (online), 13 July 2007, <www.smh.com.au>.

members, 50% of whom were over the age of 25.[42] A survey of 2,000 working adults in the United States indicated that just under half participated in online social networking, and over half of these participants were older than 35.[43]

67.56 Many individuals and organisations seeking to promote themselves in the online environment also participate in prominent online social networks. For example, in 2007, following the lead of presidential candidates in the United States, Australian politicians were encouraged to develop their own MySpace profiles to engage better with younger voters.[44]

Privacy and online social networking

67.57 Social networking websites generally enable members to create personal profiles. These can include text, photographs and video images, and often contain personal information. One concern about social networking is that it often involves participants disclosing personal information to a worldwide audience. This concern is highlighted when children and young people disclose personal information when participating in online social networking, given their more limited capacity to understand the consequences of disclosure of personal information in an online environment.[45]

67.58 There is evidence to suggest that young people use social networking websites differently to older people. In 2007, research conducted in the United Kingdom on behalf of the social network Viadeo revealed that adults aged 18–24 were more likely to post information about themselves online than those in older age groups.[46] Fifty four per cent of adults aged 18–24 indicated that other people had posted information about them online, either with or without their consent. This information then becomes part of a person's 'NetRep'—a personal online brand that others contribute to with or without consent. The Viadeo research is consistent with some of the research discussed above which indicates that those in their late teens and early 20s are more likely than any other age group to disclose personal information in the online environment.

67.59 There are concerns that participants in online social networking may be exposing themselves to dangers such as commercial exploitation, sexual predation and identity theft. In addition to chat rooms, there are now concerns that social networking

---

42 A Moses, 'Pollies Chase the Youth Vote on MySpace', *Sydney Morning Herald* (online), 29 May 2007, <www.smh.com.au>.

43 'Social Networkers Disclose Too Much Personal Info, Says CA', *OUT-LAW* (online), 9 October 2006, <www.out-law.com>.

44 A Moses, 'Pollies Chase the Youth Vote on MySpace', *Sydney Morning Herald* (online), 29 May 2007, <www.smh.com.au>; C Walters, 'Kevin, 49, Seeks Friends He Can Count', *Sydney Morning Herald* (online), 13 July 2007, <www.smh.com.au>.

45 See Ch 68 for a discussion on decision-making capacity and brain development of children and young people.

46 YouGov, *What Does Your NetRep Say About You? [Research Commissioned by Viadeo]* (2007).

websites are being used by sexual predators.[47] Children and young people are generally attuned to 'stranger danger' in chat rooms. The ALRC's consultations in this Inquiry indicated, however, that not all young people are aware that the world of social networking is a public one that may be dangerous.

67.60 Online social networking raises two main issues for consideration. The first is the extent to which young people should be able to choose to disclose information about themselves online. This chapter focuses on this issue. The second is the ability of third parties to post, alter or remove personal information about others in the online environment. This is discussed in Chapter 11.

Choosing to disclose

67.61 Many commentators (and parents) have lamented the fact that young people post large amounts of detailed personal information about themselves on websites. As one commentator remarked, this is the first generation to have their 'sexual adventures, drug taking, immature opinions and personal photographs … indelibly recorded electronically'.[48] It is now typical for young people to explore their identities by posting personal information—such as personal musings, philosophies, opinions, photographs and descriptions of everyday events in their lives—online.[49]

67.62 This does not mean, however, that young people do not value privacy. The research projects discussed above, and the ALRC's own consultations, reveal that young people value the ability to choose to disclose information about themselves. This is seen as an important aspect of privacy. A recent United States study of teenage use of social networks, which focused on privacy issues, found that many teenagers are more conscious of privacy issues than some commentators have acknowledged.

> Most teenagers are taking steps to protect themselves from the most obvious areas of risk. The new survey shows that many youth actively manage their personal information as they perform a balancing act between keeping some important pieces of information confined to their network of trusted friends and, at the same time, participating in a new, exciting process of creating content for their profiles and

---

47 In an attempt to address these concerns, New South Wales passed laws in 2007 that require convicted sex offenders to provide police with all of their active electronic communication identifiers, details of their internet service providers, and details of their internet service type. Convicted sex offenders are also required to notify police of any changes to those details, including all their active email addresses, chat room identities, and landline and mobile telephone numbers: *Child Protection (Offenders Registration) Amendment Act 2007* (NSW). A consultative working group was established by the Australian Government in September 2007 to address issues about potential abuse of social networking websites by sex offenders: H Coonan (Minister for Communications, Information Technology and the Arts) and D Johnston (Minister for Justice and Customs), 'NetAlert—Working Group Convened to Prevent Predation through Social Networking Sites' (Press Release, 13 September 2007).

48 P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

49 J Wyn and others, *Young People, Wellbeing and Communication Technologies [Prepared for Victorian Health Promotion Foundation]* (2005) Youth Research Centre, University of Melbourne, 14–17.

> making new friends. Most teens believe some information seems acceptable—even desirable—to share, while other information needs to be protected.[50]

67.63 The desire of young people to control the disclosure of their personal information is reflected in the reaction of members of a popular social networking website to certain features added to the website. In 2006, Facebook introduced a feature which automatically broadcasted changes made to a member's profile to the member's 'friends'. In 2007 it introduced a similar feature known as the 'Beacon' feature, which automatically broadcasted purchases made by a member to the member's 'friends'.[51] Facebook members threatened to boycott the website when these features were introduced. In both cases, Facebook added controls to enable members to opt out of the automatic broadcast systems. Facebook's chief privacy officer, Chris Kelly, has been quoted as saying that the classic notion of the right of privacy as the right 'to be left alone' has changed to the notion of 'I want control over my information'.[52]

67.64 It has been noted that it also is important to enable a person to change his or her mind about the disclosure of his or her personal information.[53] It is not easy, however, to remove permanently personal information posted on the internet.

> The potential harm from out-of-date, conflicting and inaccurate information on the Web is amplified by the fact that internet search engines such as Google store or cache Webpages which makes the information available online even after the author has removed the information in question. This makes it very difficult to remove or correct wrong or compromising information, which could be harmful to a person's career chances.[54]

67.65 The 2007 survey conducted for Viadeo, discussed above, asked recruitment managers and directors whether they used personal information on websites to inform recruitment decisions. While only 18% of respondents indicated they had found information about a prospective employee online, 59% of these said that it had affected their decision whether to employ the person. Fifteen per cent indicated that the information had a negative effect on their decision.[55] There also have been media reports of people failing to obtain jobs because of the disclosure of their personal

---

50 A Lenhart and M Madden, *Teens, Privacy & Online Social Networks* (2007) Pew Internet & American Life Project, i–ii.

51 K Coughlin, 'Facebook's Facelife Uncovers What Many See as Flaws: Social Networking Sites' Mainstream Aspirations are Turning Off Purists', *Times-Picayune* (online), 5 November 2006, <www.timespicayune.com>; 'Facebook Apologizes for Ad Platform "Mistakes"', *Sydney Morning Herald* (online), 6 December 2007, <www.smh.com.au>.

52 'Facebook Banks on Privacy', *Sydney Morning Herald* (online), 16 July 2007, <www.smh.com.au>.

53 P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

54 YouGov, *What Does Your NetRep Say About You? [Research Commissioned by Viadeo]* (2007), 6.

55 Ibid, 4.

information on the internet.[56] Some of the young people consulted by the ALRC reported that they had been disciplined as a consequence of their online activity.

Regulatory options

67.66 Some legislators and commentators have considered ways to eliminate, or at least alleviate, the problems associated with the disclosure of personal information by children and young people engaging in social networking.

67.67 It should be noted that many of the social networking websites are restricted to members of a certain age. For example, the most popular social networking website, MySpace, requires users to be aged 14 or over before establishing a profile. The profiles of members believed to be under 14 years of age may be deleted[57] and many of the tips to users and parents encourage the reporting of under-age profiles. Membership of Facebook was originally only open to high school and college students. It is now, however, open to any high school or college student aged between 13 and 17, and to any person over the age of 18. The profiles of under-age Facebook users may also be deleted.[58] Young people with whom the ALRC consulted indicated that these age profiles are regularly ignored by young people who lie about their age when joining these social networks. The joke was made that there are many 99 year olds with profiles on social networking websites.

67.68 As discussed in Chapter 69, the *Children's Online Privacy Protection Act* (US) (COPPA) applies to operators of commercial websites and online services directed to children under the age of 13 that collect personal information from children; and to operators of websites who are aware that they are collecting information from children under the age of 13. COPPA requires these website operators to provide notice to parents and obtain verifiable parental consent before collecting personal information from a child under the age of 13.

67.69 The Federal Trade Commission (FTC), which enforces COPPA, has a 'sliding scale' approach to obtaining verifiable parental consent. The requirements for obtaining consent are more rigorous if the intended use of the information involves disclosure to third parties. Where the information is to be used for internal purposes only, verifiable parental consent can be obtained through the use of an email message to the parent, coupled with additional steps to provide assurances that the person providing the consent is, in fact, the parent. More rigorous methods specified include: fax- or mail-back forms; credit card transactions; staffed toll-free numbers; digital certificates using public key cryptography; and emails accompanied by Personal Identification Numbers or passwords. While COPPA has been considered largely a

---

56 See, eg, M Mann, 'Some Job Hunters are What They Post', *National Law Journal* (online), 9 May 2007, <www.law.com>.

57 MySpace, *MySpace.com Terms of Use Agreement* (2008) <www.myspace.com> at 5 May 2008.

58 Facebook, *Terms of Use* (2007) <www.facebook.com> at 5 May 2008.

successful measure,[59] there has been criticism that its age verification mechanisms are easy to circumvent.[60]

67.70 One commentator has suggested that the introduction of legislation like COPPA, with a higher age barrier, would be an appropriate way to regulate social networking websites.[61] COPPA has been used to alter the practices of a number of social networking websites. Xanga.com was penalised US$1 million for collecting, using and disclosing personal information from children under the age of 13 without first notifying parents and obtaining their consent. The consent order imposed on Xanga.com by the FTC, which sets out steps to be taken to comply with COPPA, is considered to be 'best practice' for social networking websites.[62] It includes a requirement that the website operators place links to information about protecting children's online privacy in privacy policies on websites, information collection points on websites, and in notices sent directly to parents.

67.71 A number of legislators in the United States have sought to introduce legislation to prohibit or limit the access of young people to social networking websites. Bills seeking to prohibit unsupervised student access to social networking websites in schools and libraries are presently before the United States Congress.[63] A number of states in the United States have passed or proposed laws requiring social networking website operators to verify the age of every user and to obtain parental permission for the participation of those under the age of 18. The effectiveness of these proposals has been questioned, given the absence of effective online age verification mechanisms.[64] To provide any form of protection, the verification mechanism must involve more than an assumption that the user is honestly disclosing his or her age.[65]

67.72 It is also debatable whether stopping young people from engaging in online social networking is the most appropriate regulatory approach. Online social networks have become an integral part of the way in which young people express themselves and communicate with each other. One commentator has argued that:

---

59 See discussion in Ch 69.

60 M Hersh, 'Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet' (2001) 28 *Fordham Urban Law Journal* 1831, 1870.

61 H Valetk, 'Playing with Privacy: Virtual Communities Raise New Questions', *Law.com* (online), 24 May 2007, <www.law.com>.

62 *Consent Decree and Order for Civil Penalties, Injunction and Other Relief—United States v Xanga.com*, September 2006; R Urbach, 'FTC Tackles Social Networking', *DMNews* (online), 21 November 2006, <www.dmnews.com>.

63 See Deleting Online Predators Act of 2007 HR 1120 IH (US) and Protecting Children in the 21st Century Act S 49 IS (US).

64 H Valetk, 'Playing with Privacy: Virtual Communities Raise New Questions', *Law.com* (online), 24 May 2007, <www.law.com>.

65 Age verification and parental consent verification mechanisms are discussed further in Ch 68.

> Before we can solve the social networking dilemma, we must first grasp the cultural nuances of virtual communities and the potential implications of any new proposals. Otherwise, our rush to respond may fail to fully address those important concerns.[66]

67.73 A self-regulatory approach is another option. In April 2008, the United Kingdom Home Office Task Force on Child Protection on the Internet released *Good Practice Guidelines for the Providers of Social Networking and Other Use Interactive Services*. The Task Force included representatives from the internet and telecommunications industries—including representatives from MySpace, Facebook, Google/YouTube and Bebo—as well as representatives from law enforcement agencies, children's charities and government. Some of these representatives were from outside the United Kingdom. The Australian Communications and Media Authority (ACMA) participated in the Task Force. On release of the Guidelines, the Chairman of ACMA, Chris Chapman, noted the importance of providing a global safety net for children and young people who use the internet.

> I continue to be of the view that international co-operation will be increasingly the way to ensure children have a positive and safe experience of the internet and applications that utilise it—which is why the Australian Communications and Media Authority allocates a very meaningful portion of its resources to supporting practical international collaborations …[67]

67.74 While encouraging children and young people to make use of social networking services, the Guidelines focus on ensuring that children and young people understand the importance of protecting themselves, their online identities and their reputations. The Guidelines include background on social networking services and issues arising from their use; recommendations to social networking services; and safety tips for parents, carers, and children and young people. The Guidelines recommend that social networking services:

- set the default for full profiles to 'private' or to the user's approved contact list for those registering under the age of 18;
- encourage users not to disclose excessive personal data;
- clearly inform users of the options they have to adjust privacy settings, manage 'who sees what' and control whom they interact with; and
- ensure that private profiles of users under the age of 18 are not searchable either on the service or via search engines.[68]

---

66 H Valetk, 'Playing with Privacy: Virtual Communities Raise New Questions', *Law.com* (online), 24 May 2007, <www.law.com>.

67 Australian Communications and Media Authority, 'ACMA Welcomes Release of International Guideline for Safer Online Networking' (Press Release, 3 April 2008).

68 United Kingdom Home Office Task Force on Child Protection on the Internet, *Good Practice Guidelines for the Providers of Social Networking and Other User Interactive Services* (2008), 24–32.

67.75 The Guidelines discuss the use of identity authentication and age verification technologies. They note that effective technologies are still in development, but encourage the implementation of suitable solutions, to the extent legally and technically feasible, to create a safer and more secure internet environment for children and younger users.[69]

The need for education

67.76 American academics Dr Ilene Berson and Dr Michael Berson have written extensively on the protection of children's privacy in the digital age. They argue that there is a need to teach children 'digital literacy'—that is, 'the skills that people need to understand and constructively navigate the digital media that surrounds them'.[70] They note that children learn to interact in digital spaces at an early age, and that the proliferation of personal information online, including personal information about the child published by the parent, has desensitised young people to privacy issues. Accordingly, children remain oblivious to ways to maximise privacy in their online activities.[71] Digital literacy 'addresses safety and security while fostering broader preparation for digitized and networked environments'.[72]

67.77 Berson and Berson note that while young people are often proficient in using the tools of the digital world, 'they have typically not acquired the proficiency to function responsibly as members of networked communities'.[73] An important element of learning to apply critical analysis skills and make ethical decisions in this environment is to control disclosure of personal information. One study has found that children aged six to 12 are more likely than adults to click on website ads, believing they are part of the website's content.[74] Young people are learning their online social networking skills primarily from peers, and peers do not always know or pass on the important safety and privacy awareness tips that need to be learned. While it is clear that the technical skills are being learned, it is questionable whether the decision-making skills are being developed effectively before too many mistakes are made.

67.78 Children and young people may not be aware of privacy concerns surrounding the disclosure of personal information online. Many young people are surprised when they are informed that schools, police, parents and employers may be reading their online profiles. This may be because they do not think of the internet as a public place,

---

69 Ibid, 28–29. See also 'MySpace Touts New Safety Measures for Teens', *Sydney Morning Herald* (online), 15 January 2008, <www.smh.com.au>.

70 I Berson and M Berson, 'Children and Their Digital Dossiers: Lesson in Privacy Right in the Digital Age' (2006) 21 *International Journal of Social Education* 135, 142.

71 Ibid, 141.

72 Ibid, 142.

73 Ibid, 142.

74 C Albanesius, 'Teens Don't Understand Privacy Policies', *PC Magazine* (online), 10 April 2008, <www.pcmag.com>.

or of their personal profile as a highly accessible, public document.[75] Even where websites provide privacy control options for profiles (and many do), many young people choose a public profile in order to maximise their potential for making friends, not necessarily understanding the reality of what it means to be 'public' on the internet. Others are knowingly using social networking websites for self-promotion—but again, some question whether that self-promotion is undertaken with a full, mature understanding of the consequences. As one commentator has noted, 'the teenagers chattering away online are media literate, but they are not media wise'.[76]

67.79 A reliance on parental teaching on this topic may not be sufficient. Many adults do not understand adequately their privacy rights.[77] Further, although many adults are now using social networking websites, they are often less sophisticated about privacy in this environment than even their younger counterparts.[78]

67.80 The need to provide information to children, young people and their parents about the operation of the online environment has been acknowledged in Australia. A number of Australian websites provide information—and in some cases software tools—to assist with controlling privacy in the online environment.[79] ACMA provides advice and guidance to children, young people and parents on a number of telecommunications issues, such as safe use of mobile chat services.[80]

67.81 A body that has been influential in the development of educational material for the online environment is NetAlert. Established in 1999 by the Australian Government, it was a not-for-profit community organisation that provided advice and education on internet safety issues. No longer a separate entity, NetAlert continues to exist as an internet safety initiative under the management of ACMA and the Department of Broadband, Communications and Digital Economy (DBCDE). ACMA conducts the NetAlert Outreach and Research program, which provides information on current trends in internet safety and undertakes targeted awareness-raising campaigns and activities.[81] The DBCDE manages the *NetAlert—Protecting Australian Families*

---

75 C Thomas, 'Kids Think Posting Online is Private, Say Educators', *Hamilton Spectator* (online), 1 May 2007, <www.hamiltonspectator.com>; S Steinbach and L Deavers, 'The Brave New World of MySpace and Facebook', *Inside Higher Ed* (online), 3 April 2007, <insidehighered.com>.

76 P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

77 In the 2004 Australian survey of community attitudes to privacy, 35% indicated they had some level of knowledge, 34% indicated very little, and 4% said they had no knowledge of their rights when it comes to protecting personal information—only 22% indicated they had an adequate amount of knowledge, and 4% said they had a lot of knowledge: Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), 11. This question was not asked in the 2007 survey, although generally awareness of federal privacy laws has increased: Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), 6.

78 See, eg, D Devlin, 'Baby Pics on the Net: Public or Private?' *Yahoo? Tech* (online), 30 May 2007, <tech.yahoo.com/blogs/devlin/11228> and comments posted on that website.

79 See Ch 9 for a full discussion of privacy-enhancing tools for the online environment.

80 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

81 NetAlert, *About NetAlert* <www.netalert.gov.au/about_netalert.html> at 14 April 2008.

Online initiative, a particular package focused on child safety in the online environment.

67.82 In addition to information for parents and teachers, the NetAlert website includes a number of interactive educational programs on internet safety, including: Netty's World aimed at young children to age 7; CyberQuoll aimed at upper primary school students; Cybernetrix aimed at secondary school students; and Wise Up To IT aimed at young people aged 16 and over.[82] The educational materials are of high quality, and in an age-appropriate way cover topics such as inappropriate internet content, cyber bullying, stalking and paedophile activity, computer security, and identity theft. All of the material focuses on the dangers of chat websites, but has not yet addressed the newer realities of social networking websites.[83] CyberQuoll, for example, provides a good scenario on the dangers of posting photographs online, and considers the consequences of peer use of the photographs as well as paedophile activity. At present, the Cybernetrix program for the older age group does not give much information on social networking websites, although it does alert young people to the dangers of providing personal information online and provides links to the OPC website. The Wise Up To IT website has a more limited breadth of material.

67.83 Specific educational material about social networking websites is beginning to appear in Australia and overseas. Many of the social networking websites themselves include tips and suggestions for controlling privacy of individual profiles, but privacy commissioners around the world are now producing and publishing their own educational material on social networking. Some of the initiatives have included:

- a pamphlet for college students developed by the Information and Privacy Commissioner of Ontario, in conjunction with Facebook, about selecting and using social networking websites;[84]

- a special website developed by the United Kingdom Information Commissioner's Office for young people which focuses on online social networking;[85] and

---

82 All of the websites are linked from NetAlert, *Website* <www.netalert.com.au> at 14 April 2008.

83 However, the NetAlert website contains some information on social networking websites, including some safety tips: NetAlert, *Social Networking* <www.netalert.gov.au/advice/services/social_networking.html> at 14 April 2008.

84 Information and Privacy Commissioner of Ontario, 'Think About Your Privacy When Selecting a Social Networking Site: Commissioner Cavoukian' (Press Release, 12 October 2006). See also brochure Information and Privacy Commissioner of Ontario and Facebook, *When Online Gets Out of Line—Privacy: Make an Informed Online Choice [pamphlet]* (2006). At the time the pamphlet was developed, college students were the main users of Facebook.

85 United Kingdom Information Commissioner's Office, *Welcome to the ICO Pages for Young People* (2007) <www.ico.gov.uk/youth.aspx> at 15 April 2008.

- a series of frequently asked questions on the issue of privacy and social networking websites, including links to other websites providing information and assistance on social networking, developed by the OPC and published on its website.[86]

Discussion Paper proposals

Research on attitudes to privacy

67.84 In DP 72, the ALRC noted that better research on attitudes to privacy was needed to support evidence-based policy making in the future. The ALRC proposed that the Australian Government fund a longitudinal study of the attitudes of Australians to privacy.[87]

67.85 There was strong support for the proposed longitudinal study.[88] The Public Interest Advocacy Centre noted that the study would differ from the cross-sectional attitudinal surveys previously undertaken by the OPC because it would examine changes in the attitudes of individuals over a period of time.[89] The OPC listed many of the benefits that could be gained from the research that would enhance the role of the OPC. It disagreed, however, with the ALRC's view that it was not the appropriate body to conduct such a study. It submitted that it should play a central part in the overall management of the study and, in particular, that it should have strategic input into the study at the planning stages.[90]

Privacy education for children and young people

67.86 In DP 72, the ALRC indicated that it did not propose the regulation of the practice of online social networking. Instead, the ALRC expressed the view that children, young people, teachers and parents should be educated about social networking websites. This education should highlight the dangers associated with online social networking, and provide advice on how to use social networking websites safely and appropriately.[91]

---

86 Office of the Privacy Commissioner, *Your Privacy Rights: FAQs—Social Networking* <www.privacy.gov.au/faqs/ypr/#social_networking> at 14 April 2008. This information was first published in December 2007.

87 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 59–1.

88 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007.

89 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

90 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

91 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [59.111].

67.87 The ALRC noted that concerns about the privacy practices of children and young people in the online environment reflected a broader concern about the lack of awareness of children and young people of privacy issues and laws. The ALRC made a number of proposals aimed at developing and delivering educational material on privacy to children and young people. It proposed that:

- the OPC should develop and publish educational material about privacy issues aimed at children and young people;[92]

- NetAlert should include specific guidance on using social networking websites as part of its educational material on internet safety;[93] and

- state and territory education departments should incorporate education about privacy, and in particular privacy in the online environment, into school curriculums.[94]

67.88 Few stakeholders commented on the ALRC's view that it was not appropriate to attempt to regulate online social networking. The Law Society of New South Wales agreed with it, noting that rapid changes in internet-based technology would mean any regulatory measures would be outdated and obsolete within a short time frame, possibly even before the measures came into force.[95]

67.89 There was strong support for the ALRC's privacy education proposals.[96] The OPC supported the proposal that it develop and publish educational material about privacy issues aimed at children and young people.[97] Medicare Australia also supported the proposal, particularly if the material addressed issues that arise in the

---

92 Ibid, Proposal 59–2.

93 Ibid, Proposal 59–3.

94 Ibid, Proposal 59–4.

95 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

96 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; ASTRA, *Submission PR 426*, 7 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007

97 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

context of the handling of children and young people's health and claims information.[98]

67.90 A number of stakeholders commented specifically on the need for education about privacy in the online environment. The Australasian Compliance Institute commented that:

> An education campaign would be appropriate particularly around the possible detriment or damage to reputation that a young person could potentially suffer in the long term if certain personal information is divulged then, for example, as adults, they later find themselves in the public eye, or in positions where fitness and propriety requirements have to be satisfied. This will also assist with other concerns in relation to young people for instance, identity theft, predatory behaviour and personal safety.[99]

67.91 ACMA agreed with the proposal to extend the role of the NetAlert scheme to cover social networking, and noted that strong partnerships between government, industry and community sectors are essential to ensure that the message of educational campaigns about privacy is effectively communicated.[100]

ALRC's view

A longitudinal study of attitudes to privacy

67.92 The *Privacy Act* is based largely on the recommendations of a previous ALRC inquiry into privacy conducted in the late 1970s and early 1980s. The current Inquiry is being conducted in a very different world where: technology has greatly changed the way in which we hold and exchange information; governments have contracted out a wide range of services; and the threat of terrorism has placed security concerns high on the public agenda. There is limited Australian research upon which to draw in order to determine whether expectations of privacy have changed since the ALRC's previous inquiry.

67.93 The privacy concerns of children and young people, however, do appear to differ from those of older Australians. For example, in general young people appear more prepared than older people to accept government interference with privacy rights in the name of the public good. In addition, young people appear to have different views to older people about the regulation of privacy in the online environment. They appear to be more aware than older people of the difficulties associated with the regulation of activities on the internet, perhaps because of their familiarity with the online environment. Young people have suggested that promoting individual control of personal information in the online environment is more appropriate than attempting to impose technical legal rules on internet users.

---

98 Medicare Australia, *Submission PR 534*, 21 December 2007.

99 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007. See also Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

100 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

67.94 These differences in the views of young people and adults about privacy are not so great as to warrant a reconsideration of the basic framework of the *Privacy Act*. In the ALRC's view, the existing framework of the *Privacy Act*, reformed in accordance with the recommendations in this Report, reflects adequately the privacy expectations of children and young people in Australia. Many of the recommended changes to the privacy framework in Australia are aimed at improving the clarity, consistency and enforcement of privacy laws. These changes will be of benefit to all Australians, and are also consistent with the expectations of young Australians.

67.95 To date, the surveys commissioned by the OPC have provided useful information on community attitudes to privacy. They are not a substitute, however, for a proper longitudinal study encompassing both quantitative and qualitative research on privacy. Qualitative research, while more difficult to conduct and analyse, is more likely to explain experiences and beliefs in terms of the wider contexts of peoples' lives. A longitudinal study will help to determine whether the attitudes of Generation Y today will persist over time or whether they are attributable to youth more generally, and whether generations that follow will have different attitudes to privacy.

67.96 The ALRC recommends, therefore, that the Australian Government fund a longitudinal study of the attitudes of Australians to privacy. The study should be representative of the Australian population, and should include participants under the age of 18.

67.97 Given that the outcomes of the research will be directly relevant to national policy development, funding for the project should be provided by the Australian Government. Although noting the OPC's disagreement on this point, the ALRC does not consider that the OPC is the appropriate body to conduct or direct a longitudinal study. Given the OPC's experience with surveys about attitudes to privacy, it would be useful and appropriate for it to have input into the planning and design of the study.

67.98 A number of existing Australian Government research bodies, in particular the Australian Institute of Health and Welfare and the Australian Institute of Family Studies, have the capacity and experience to undertake longitudinal studies of this kind, although their functions do not usually extend to information and statistics on privacy. Funding could be made available to appropriate academic researchers through the Australian Research Council. Alternatively, the Government may fund an appropriate researcher or research body directly to undertake this project.

Recommendation 67–1 The Australian Government should fund a longitudinal study of the attitudes of Australians, in particular young Australians, to privacy.

Online social networking

67.99 As noted above, there are concerns about the way in which young people use social networking websites. Consistent with its approach to online regulation generally,[101] the ALRC is not making a recommendation to regulate such websites. The ALRC, however, does make recommendations in Chapter 68 to ensure that decisions under the *Privacy Act* regarding the personal information of children and young people under the age of 15 are made by people with parental responsibility for the child or young person.

67.100 The ALRC notes that many social networking websites are setting age limits on membership. Further, online social network providers are encouraging parental monitoring and reporting of under-age use of their websites. The *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services*,[102] which was developed with input from major social networking websites, is a useful global initiative that may have an impact of the way in which this industry develops. While initiatives like these are to be encouraged, they are unlikely to stop curious children and young people from avoiding simple age verification mechanisms online and continuing to make bad privacy choices when interacting via the internet.

67.101 The ALRC considers that the most effective measure that can be taken at present is to educate children, young people, teachers and parents about social networking websites. Education in this area should highlight the privacy dangers associated with the disclosure of personal information on social networking websites and should provide advice on how to use these websites safely and appropriately.

Privacy education for children and young people

67.102 Children and young people need to be informed and educated about privacy issues so that they are better equipped to protect their own privacy and respect the privacy of others. Education programs should focus on privacy issues that arise in the online environment, and in interactions with government, organisations and other individuals. Education initiatives aimed at young people can improve the behaviour of adults in the next 10–15 years, and also may educate parents through a 'trickle up effect'.[103] The recommendations below are intended to equip young people with the necessary information and analytical skills to make appropriate decisions about withholding or disclosing personal information in different circumstances.

---

101 See Ch 11.

102 United Kingdom Home Office Task Force on Child Protection on the Internet, *Good Practice Guidelines for the Providers of Social Networking and Other User Interactive Services* (2008).

103 Workshop Summary, 'Workshop: Children's Privacy Education' (Paper presented at Terra Incognita: Privacy Horizons—29th International Conference of Data Protection and Privacy Commissioners, Ottawa, 28 September 2007).

67.103 The Human Rights and Equal Opportunity Commission provides a range of resources on its website for students. Resources are also available to assist teachers to incorporate human rights issues and case studies into lesson plans.[104] The OPC presently has a range of web pages and information sheets that provide guidance to individuals on the operation of the *Privacy Act*. This material is not, however, aimed specifically at children and young people.

67.104 The ALRC recommends that the OPC develop and publish education material aimed specifically at a younger audience, and geared towards school curriculums. This will make the information in the materials more accessible to children and young people. The incorporation of OPC materials into student lessons also may help to raise the profile of the OPC among young people, better enabling them to obtain access to further information about privacy and to utilise the complaint-handling processes available to them.

67.105 There also is a need for educational material dealing specifically with privacy issues associated with online social networking. The NetAlert brand, which is now administered by ACMA, is already used extensively in the school and home environment, and it would be a good vehicle for ensuring that children and young people are introduced to the relevant safety and privacy issues in social networking environments. The ALRC recommends that the OPC and ACMA work together to update existing educational material, or create new material, about privacy issues in online social networking for a range of age groups.

67.106 While the development of educational material, and any accompanying educational campaigns run by the OPC and ACMA, will improve greatly the quality of information available about privacy issues, the ALRC still considers that there is a need to bring these issues to the attention of children and young people in a more systematic way. The ALRC recommends, therefore, that education about privacy rights, the protection of personal information, and respect for the privacy of others, be incorporated into school curriculums. Privacy issues should be discussed in lessons about computers and online safety, some commerce and legal studies lessons, and generally in education about civics and citizenship. Teachers should be able to draw on educational materials recommended in this chapter, as well as existing material available online. An introduction to these issues within the school environment will help to equip young people with the necessary skills to identify and manage privacy and safety issues.

---

104 Human Rights and Equal Opportunity Commission, *Education* <www.humanrights.gov.au/education/index.html> at 22 May 2008.

Recommendation 67–2 The Office of the Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people.

Recommendation 67–3 The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority, should ensure that specific guidance on the privacy aspects of using social networking websites is developed and incorporated into publicly available educational material.

Recommendation 67–4 In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, including privacy in the online environment, into school curriculums.

68. Decision Making by and for Individuals Under the Age of 18

Contents

Introduction

68.1 There is no federal legislation specifically addressing the privacy of children and young people. While the *Privacy Act 1988* (Cth) applies to individuals under the age of 18, there is no provision dealing explicitly with the particular needs of children and young people. It is not always clear how the Act applies to these individuals, or who

can and should make decisions about privacy on behalf of an individual under the age of 18.

68.2 The need for the *Privacy Act* to address children's privacy was discussed at the time of passage of the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Opposition moved amendments that would require a 'commercial service' to obtain the consent of a child's parent before collecting, using or disclosing personal information concerning a child aged 13 or under.[1] While the amendment was not agreed to, the Government indicated that the issue would be investigated further.[2]

68.3 In 2001, the then Attorney-General, the Hon Daryl Williams MP, announced the establishment of a consultative group on children's privacy, convened by the Attorney-General's Department.[3] The consultative group met twice, but despite plans for publication of a discussion paper on children's privacy, the matter was not progressed.[4]

68.4 Children's privacy was exempted specifically from the review of the private sector provisions of the *Privacy Act* that was completed by the Office of the Privacy Commissioner (OPC) in 2005.[5] The 2005 review of the *Privacy Act* by the Senate Legal and Constitutional References Committee did not examine the issue of children's privacy.[6]

68.5 This Inquiry has provided the first opportunity to undertake a comprehensive examination of issues relating to the privacy of children and young people. In this chapter, the ALRC considers a number of issues about decision making by and for individuals under the age of 18, and what, if any, changes are needed in the *Privacy Act* or other legislation. Generally, the ALRC supports the existing approach that individuals under the age of 18 should be assessed individually to determine whether they have the capacity under the Act to make a decision. The ALRC also recommends a range of mechanisms, including guidance from the OPC and training for staff in agencies and organisations, aimed at ensuring that appropriate assessments are undertaken.

---

1 The amendment was headed 'Special protection for children': Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2006, 20302 (N Bolkus). The amendment was supported by the Australian Democrats: Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 November 2000, 20162 (N Stott Despoja), 20165.

2 The Government acknowledged that the notion of children's privacy had merit, but that the form of the amendment needed consultation before it could be accepted: Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2000, 20304 (A Vanstone—Minister for Justice and Customs).

3 D Williams (Attorney-General), 'First Meeting of Consultative Group on Children's Privacy' (Press Release, 4 June 2001).

4 Australian Government Attorney-General's Department, *Children's Privacy* (2000) <www.ag.gov.au/www/agd/agd.nsf/Page/Privacy_Privatesectorprivacy_ChildrensPrivacy> at 10 April 2008.

5 The terms of reference for that review stated that children's privacy was one of 'certain aspects of the private sector provisions [which] are currently, or have recently substantively been, the subject of separate review': Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 22, App 1.

6 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

68.6 The ALRC also has recognised, however, that there are many situations where individual assessment is not reasonable or practicable, and recommends that, in the absence of an individual assessment, there be an age at which an individual is presumed to have capacity to make a decision on his or her own. After considering the latest research on child development and the brain development of adolescents, and community debates about ages of capacity, the ALRC recommends that the age be set at 15. Below this age, it is recommended that an individual who has not been assessed individually should be considered incapable of making a decision under the *Privacy Act*. The ALRC recommends a number of new provisions for the *Privacy Act* to implement this policy, and to define who is capable of making a decision on behalf of an individual who is not capable of making a decision under the Act.

68.7 In Chapter 69, the ALRC considers a number of areas where specific privacy issues concerning children and young people arise.

Privacy rights of children and young people at international law

68.8 Chapter 1 notes the recognition of privacy as a human right in a number of international conventions. The specific right of privacy for children also is set out in art 16 of the United Nations *Convention on the Rights of the Child 1989* (CROC).[7]

> 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
>
> 2. The child has the right to the protection of the law against such interference or attacks.

In addition, art 40(2)(b)(vii) of CROC refers to the specific need to have respect for the privacy of a child accused or found guilty of a criminal offence.

68.9 The articles of CROC deal with information privacy, including such things as rights to confidential advice and counselling, and control of access to information stored about the child in records. The articles also have been interpreted to cover 'privacy' in terms of physical environment and the privacy of relationships and communications with others.[8] For example, a concern of the United Nations Committee on the Rights of the Child is the personal space provided to, and the

---

7 *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990). 'Child' is defined in the Convention as a person under the age of 18.

8 UNICEF, *Implementation Handbook for the Convention on the Rights of the Child* (fully revised ed, 2002).

regulation of communications of, children and young people in institutional care, including in juvenile justice facilities and immigration detention.[9]

68.10 CROC was adopted by the United Nations in November 1989 and ratified by Australia in December 1990, coming into effect in Australia in January 1991.[10] It is the most universally accepted international convention.[11] Any federal, state or territory legislation, policy or practice that is inconsistent with CROC places Australia in breach of its international obligations, and could have consequences at the international level.[12]

68.11 A number of other international guidelines relating to the rights of children make reference to the need to protect privacy, including the *United Nations Standard Minimum Rules for the Administration of Juvenile Justice 1985* (the Beijing Rules)[13] and the *United Nations Rules for the Protection of Juveniles Deprived of Their Liberty 1990*.[14] Although not necessarily binding on Australia at international law, these rules represent internationally accepted minimum standards and are important reference points in developing policy.

68.12 CROC has aroused significant misgivings within some sections of the Australian community, and in other countries, about the interaction between the rights of children and governments and the rights of parents to raise their family in the way they believe to be most appropriate.[15] These concerns also were present during the drafting of the Convention, and led to the inclusion of art 5, which reads:

---

9 J Doek—Chairperson UN Committee on the Rights of the Child, *Consultation PM 14*, Sydney, 18 August 2006.

10 While CROC has been ratified by Australia, it has not been fully implemented into Australian domestic legislation. Australia's international law obligations are relevant to the interpretation of Australian statutes, and Australian courts generally will interpret legislation to reach a result that is inconsistent with Australia's international law obligations only if there is 'a clear indication that the legislature has directed its attention to the rights or freedoms in question, and has consciously decided upon abrogation or curtailment': *Plaintiff S157/2002 v Commonwealth* (2003) 211 CLR 476, [30]. For a detailed exposition of the influence of international law (and especially international human rights law) on Australian municipal law, see R Piotrowicz and S Kaye, *Human Rights: International and Australian Law* (2000).

11 Many countries have placed reservations and declarations on a number of articles. Australia has a reservation in relation to art 37(c) based on physical size and population distribution difficulties in ensuring the separation of young offenders and adult offenders while enabling young offenders to maintain contact with their families: Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [20.102].

12 Except in relation to art 37(c).

13 *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985). See in particular rule 8, which is discussed below in relation to access to court records.

14 *United Nations Rules for the Protection of Juveniles Deprived of Their Liberty*, UN Doc A/RES/45/113 (1990). See in particular rule 19 on records.

15 Parliament of Australia—Joint Standing Committee on Treaties, *United Nations Convention on the Rights of the Child* (1998), [1.36]; M Otlowski and B Tsamenyi, 'Parental Authority and the United Nations Convention on the Rights of the Child: Are the Fears Justified?' (1992) 6 *Australian Journal of Family Law* 137.

> States Parties shall respect the responsibility, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.

68.13 CROC embodies a balancing exercise, recognising that the family is the fundamental unit of society, but that children are individuals who are not wholly subsumed by their family. The rights set out in CROC are the rights of children which should be respected by their families, communities and governments. Article 5 clearly anticipates that, while a child should be guided appropriately by parents and others in exercising his or her rights, a child also will become more independent of family as his or her capacities develop. It is at this point—where a child becomes a young person with needs and wishes separate from his or her parents—that difficulties may arise in determining whether a child should be able to exercise rights on his or her own behalf. Article 12 of CROC, which refers to a child's right to be heard in matters affecting the child, makes a similar assumption regarding the evolving capacity of children.[16]

68.14 Consistent with CROC, most rights and responsibilities in Australian law refer to a person as an adult when he or she turns 18 years of age.[17] While historically the law has generally assumed that children do not have the capacity to participate in legal processes on their own behalf, more recent psychological studies have provided a greater understanding of children's cognitive abilities and prompted a re-evaluation of rules regarding children's capacity.[18] Increasingly, the common law and particular statutes are recognising the ability of young people at an age lower than 18 to make decisions on their own behalf, even where this may conflict with the wishes of their parents.

---

16 The article requires that 'the child who is capable of forming his or her own views' should have the right to express those views, and that the views should be 'given due weight in accordance with the age and maturity of the child': *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990) art 12(1).

17 This varies, however, particularly in the area of juvenile justice: see L Blackman, *Representing Children and Young People: A Lawyers Practice Guide* (2002), 4–5.

18 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [4.7]–[4.9]; Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [4.4]–[4.9], [14.19]–[14.24]. The research is discussed in more detail below.

Existing Australian laws relating to privacy of individuals under the age of 18

Privacy Act

68.15 The personal information of individuals under the age of 18 is regulated by a number of laws. The laws that apply will depend upon who holds the information, although generally personal information held by Commonwealth and ACT agencies or their contractors, or held by non-government bodies not otherwise exempt from the operation of the Act, is regulated by the *Privacy Act*.[19] Many of the ALRC's recommendations to streamline and clarify the operation of the *Privacy Act* and other privacy laws in Australia also will improve the handling of personal information of individuals under the age of 18.[20] In particular, the ALRC recommends that the Information Privacy Principles (IPPs) that apply to agencies, and the National Privacy Principles (NPPs) that apply to organisations, be replaced with a single set of principles, referred to in this Report as the model Unified Privacy Principles (UPPs).[21]

68.16 Many aspects of the privacy principles may require or allow an individual to provide consent to the collection, use or disclosure of personal information about him or her. The Act also establishes a number of situations where an individual can make a request or exercise a right. Each of these situations has a decision-making element. These include:

- consenting to the collection of sensitive information;[22]
- consenting to a particular use or disclosure of personal information, including consent to use such information for the purpose of direct marketing;[23]
- requesting not to receive further direct marketing communications from an organisation;[24]
- consenting to the transfer of personal information outside of Australia;[25]
- requesting access to personal information held by an agency or organisation;[26]

---

19 For a more detailed analysis of the scope of existing privacy laws in Australia, see Ch 2.

20 These recommendations include adoption of nationally consistent privacy laws across jurisdictions (Ch 3), amendment of the Act to achieve greater logical consistency, simplicity and clarity (Rec 5–2), and inclusion of an objects clause in the Act (Rec 5–4).

21 See Rec 18–2.

22 See 'Collection' principle and discussion in Ch 21.

23 See 'Use and Disclosure' principle and 'Direct Marketing' principle and discussion in Chs 25 and 26.

24 See 'Direct Marketing' principle and discussion in Ch 26.

25 See 'Cross-Border Data Flows' principle and discussion in Ch 31.

26 See 'Access and Correction' principle and discussion in Ch 29.

- opting for anonymity or pseudonymity in transacting with an agency or organisation;[27] and

- making a complaint against an agency or organisation.[28]

68.17 A number of other requirements set out in the privacy principles aim to provide information to the individual to alert him or her to the circumstances of the collection, use and disclosure of personal information about him or her.[29] In some cases, this information will assist an individual in deciding whether to provide or withhold consent to a particular collection, use or disclosure, or to make a request under the Act.

68.18 The *Privacy Act* sets no minimum age at which an individual can make decisions regarding his or her personal information. The *Guidelines to the National Privacy Principles* suggest that each case must be considered individually, and give guidance as to when a young person may have the capacity to make a decision on his or her own behalf.

> As a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person; for example if the child is very young or lacks the maturity of understanding to do so themselves.[30]

68.19 The *Guidelines on Privacy in the Public Health Sector* stress that where a young person is capable of making his or her own decisions regarding personal information, he or she should be allowed to do so.[31] The Guidelines further suggest that, even if the young person is not competent to make a decision, his or her views should still be considered.[32]

68.20 At present, there is no structure in the *Privacy Act* for making decisions on behalf of an individual unable to make a decision concerning the privacy of his or her

---

27 See 'Anonymity and Pseudonymity' principle and discussion in Ch 20.

28 See discussion in Ch 49.

29 See, eg, 'Notification' principle, which requires an agency or organisation to take such steps, if any, as are reasonable to ensure the individual is aware of a list of factors relating to the collection and use of their personal information, and the 'Openness' principle, which requires agencies and organisations to create a Privacy Policy: Chs 23, 24.

30 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 21. Guidelines relating to the IPPs are more ambivalent, noting it may not be appropriate to rely on consent given by another person if a person under the age of 18 years is sufficiently old and mature to consent on their own behalf: Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996), 29.

31 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 33.

32 Ibid, 34.

personal information.[33] It is assumed that parents are responsible for making decisions on behalf of children or young people incapable of making the decision themselves.[34]

Other privacy legislation

68.21 Some states and territories have legislation or administrative practices that regulate the privacy of certain personal information held by state or territory public sector agencies.[35] Most apply specifically to health information and are discussed in more detail in Chapter 2.

68.22 Generally, these statutes and schemes adopt the same approach to children and young people as the *Privacy Act*. Individuals under the age of 18 are given the same rights and protections as adults, and there are no specific protections or additional provisions relating to children or young people.

68.23 Some state and territory legislation, however, does provide statutory guidance on when a child or young person will be considered capable of making decisions without a parent or guardian regarding his or her personal information. For example, s 85(3) of the *Health Records Act 2001* (Vic) states:

> (3) For the purposes of sub-sections (1) and (2), an individual is incapable of giving consent, making the request or exercising the right of access if he or she is incapable by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder of—
>
> (a) understanding the general nature and effect of giving the consent, making the request or exercising the right of access (as the case requires); or
>
> (b) communicating the consent or refusal of consent, making the request or personally exercising the right of access (as the case requires)—
>
> despite the provision of reasonable assistance by another person.

68.24 In the *Health Records (Privacy and Access) Act 1997* (ACT), the test of capacity is linked to the ability to understand the nature of, and give consent to, a health service.[36] Some legislation also includes express provisions on how, and by whom,

---

33 The only exception is NPP 2.4 which allows disclosure of health information to a 'responsible' third party in the event that an individual is incapable of giving or communicating consent for disclosure, and the disclosure is necessary for the care or treatment of the individual or for compassionate reasons: *Privacy Act 1988* (Cth) sch 3, NPP 2.4. The decision to disclose is made by the health care service provider. A 'responsible' person is defined to include a parent of the individual: *Privacy Act 1988* (Cth) sch 3, NPP 2.5.

34 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 213.

35 For an overview of privacy regulation in the states and territories, see Ch 2.

36 'Young person' is defined as a person under 18 years of age other than a person 'who is of sufficient age, and of sufficient mental and emotional maturity, to (a) understand the nature of a health service; and (b) give consent to a health service': *Health Records (Privacy and Access) Act 1997* (ACT) s 25, Dictionary.

decisions can be made on behalf of a child or young person unable to make his or her own decisions.[37]

Research on capacity

68.25 There is clear evidence that children differ from adults in their capacity to make decisions.[38] It is not clear, however, at what age an individual should be regarded as having the capacity to make a decision regarding his or her personal information. The following provides an overview of the research on the issue.

Ages of development

68.26 There is a general consensus in the literature on child development that the capacity of children to make voluntary and rational decisions increases with both age and the development of cognitive skills.[39] Decision making is a skill that develops over time together with the development of certain cognitive skills, including the capacity for logical thought, the ability to understand cause and effect, and the analysis of consequences of decisions. Jean Piaget, a leading child psychologist, identified four stages of cognitive development through which all children pass and the typical ages at which this development occurs.[40] It is during the fourth stage—the 'formal operations' period—that a child demonstrates adult-like thinking abilities such as a comprehension of abstract logic, a capacity to reason, the use of deductive and inductive reasoning, making of intelligent choices, and the ability to hypothesise.

68.27 Piaget's typology, including the allocation of typical ages at which certain developments occur, resonates with research about the decision-making capacities of children.[41] In her examination of the capacity of minors to provide voluntary consent to medical treatment, Dr Tara Kuther noted:

---

37 *Health Records Act 2001* (Vic) s 85(6) states that 'If the child is incapable, the giving, making or exercising of the consent, request or right may be provided by a parent or other authorised representative of the child'. Part 4 cl 4(3) of the draft *National Health Information Code* is an identical provision, and the *Health Records and Information Privacy Act 2002* (NSW) s 7 has a similar operation. *Health Records (Privacy and Access) Act 1997* (ACT) s 25, Dictionary specifies that the rights of an incapable young person are to be exercised by a parent, guardian or other person with parental responsibility.

38 See, eg, T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 349.

39 Ibid, 348. A child's competency, however, may not necessarily increase in direct relation to his or her age: S Ramsey, 'Representation of the Child in Protection Proceedings: The Determination of Decision-Making Capacity' (1983–1984) 17 *Family Law Quarterly* 287, 315.

40 D Singer and T Revenson, *A Piaget Primer: How A Child Thinks* (revised ed, 1996), 20–26. The four stages and typical ages associated with the stages are: the 'sensory motor' period (birth to two years of age); 'pre-operational' period (two to seven years of age); 'concrete operations' period (seven to 11 years of age); and 'formal operations' period (11 to 15 years of age).

41 S Ramsey, 'Representation of the Child in Protection Proceedings: The Determination of Decision-Making Capacity' (1983–1984) 17 *Family Law Quarterly* 287, 312–313.

> During the adolescent years, minors become better able to consider information and opinions from diverse sources, and capable of owning their judgements. Between the ages of 15 and 17, most adolescents become capable of providing voluntary consent that is not unduly influenced by others.[42]

68.28 Kuther also discusses the way in which children exercise more independence in making decisions as they become older. In particular she notes:

> Young children tend to view authority figures such as physicians and parents as legitimate and powerful, and are likely to comply with their requests because of differences in perceived social power. With increasing age, authority figures tend to be viewed as cooperative and orientated toward promoting social welfare; adolescents are more likely to question demands that seem unreasonable and are less susceptible to coercive influence.[43]

68.29 Many commentators argue that young people that have reached a certain age have the same capacity as adults to make decisions. The area that has received the most attention is the capacity of an individual to consent to medical treatment. In a study comparing the competency of individuals aged 9, 14, 18 and 21 to make informed decisions about medical treatment, Dr Lois Weithorn and Dr Susan Campbell found that, in general, 14 year olds demonstrated the same level of competence as those aged 18 years and over.[44] The researchers used four standards of competency to test the making of hypothetical medical decisions: evidence of choice; reasonable outcome; rational reasons; and understanding.[45] Weithorn and Campbell noted that while nine year olds were less competent to make a rational decision, even they were able to comprehend the basics of what is required of them when they are asked to state a preference for treatment.[46]

68.30 Based on her research, Kuther suggests that young people aged 15 can make decisions concerning medical treatment;[47] Sarah Ramsey suggests the age is somewhere between 14 and 16 years of age.[48]

---

42 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 348, citing C Lewis, 'Minors' Competence to Consent to Abortion' (1987) 42 *American Psychologist* 84 and T Grisso and L Vierling, 'Minors' Consent to Treatment: A Developmental Perspective' (1978) *Professional Psychology* 412.

43 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 347, citing W Damon, 'Measurement and Social Development' (1977) 6(4) *Counselling Psychologist* 13 and R Thompson, 'Vulnerability in Research: A Developmental Perspective on Research Risk' (1990) 61 *Child Development* 1.

44 L Weithorn and S Campbell, 'The Competency of Children and Adolescents to Make Informed Treatment Decisions' (1982) 53 *Child Development* 1589.

45 The four hypothetical dilemmas were diabetes, epilepsy, depression and enuresis.

46 Weithorn and Campbell cautioned, however, that their findings are limited in so far as their subjects were 'normal, white, healthy individuals of higher intelligence and middle-class background and that the situations they considered were hypothetical': L Weithorn and S Campbell, 'The Competency of Children and Adolescents to Make Informed Treatment Decisions' (1982) 53 *Child Development* 1589, 1596.

47 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 350.

48 S Ramsey, 'Representation of the Child in Protection Proceedings: The Determination of Decision-Making Capacity' (1983–1984) 17 *Family Law Quarterly* 287, 314.

68.31 Although the evidence suggests that decision-making abilities are linked to age, the evidence also suggests that it is not possible to identify an age above which *all* children are competent to make decisions and below which *all* children are not competent.

Brain development and psychosocial factors

68.32 In addition to the more traditional child development research, there is a growing body of research into the brain development of adolescents and the relationship between brain development and the capacity of adolescents to make decisions. This research does not necessarily contradict the earlier research on the stages of child development, but adds an additional element to the understanding of the process and outcomes of decision making by adolescents.

68.33 The frontal lobe of the brain is responsible for functions such as organising thoughts, setting priorities, planning and making judgments. Scientists have discovered that the frontal lobe undergoes significant change during adolescence, in which it produces a significant amount of 'grey matter' (the brain tissue responsible for thinking) and then undergoes a period in which it rapidly thins or 'prunes' the grey matter and develops 'white matter' (the brain tissue responsible for making the brain operate precisely and efficiently).[49] The research suggests that the frontal lobe, and therefore an individual's decision-making capacity, has not reached full maturity until some time in a person's early twenties.[50]

68.34 Other research looking at how different parts of the brain interrelate has led researchers to conclude that adolescents rely more heavily than adults on the parts of the brain that react to emotion than on the (more logical) frontal lobe, possibly because the frontal lobe is still maturing.[51] As a result, it has been suggested that adolescents allow their emotional responses to situations to determine their course of action and do not fully evaluate the consequences of a particular course of action before commencing

---

49 C Wallis and K Dell, 'What Makes Teens Tick', *Time Magazine* (online), 10 May 2004, <www.time.com>; J Fagan, 'Adolescents, Maturity, and the Law', *The American Prospect* (online), 14 August 2005, <www.prospect.org>; A Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center—American Bar Association, 2, citing E Sowell et al, 'In Vivo Evidence for Post-Adolescent Brain Maturation in Frontal and Striatal Regions' (1999) 2 *Nature Neuroscience* 10 and E Sowell et al, 'Mapping continued Brain Growth and Gray Matter Density Reduction in Dorsal Frontal Cortex: Inverse Relationships During Post-Adolescent Brain Maturation' (2001) 21 *Journal of Neuroscience* 22.

50 A Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center—American Bar Association, 2. See also L Bowman, *New Research Shows Stark Differences in Teen Brains* (2004) Death Penalty Information Center <www.deathpenaltyinfo.org> at 10 April 2008, 1.

51 D Yurgelun-Todd, *Inside the Teenage Brain: Interview* (2002) Public Broadcasting Services <www.pbs.org/wgbh/pages/frontline/shows/teenbrain/interviews/todd.html> at 10 April 2008.

it.[52] One study has shown that age differences in decision making and judgment become most apparent when the decisions of adolescents in emotionally charged or highly social situations are compared with the decisions of adults in similar situations. For example, it has been found that adolescents take more risks when in the presence of their peers than do adults.[53]

68.35 While some have cautioned against jumping to conclusions about adolescent decision-making capacity based on the latest brain research,[54] the findings and suggestions are consistent with a review of the studies by Elizabeth Cauffman and Professor Laurence Steinberg on the susceptibility of adolescents to influence. Cauffman and Steinberg identify three themes that emerge from research on age difference in decision-making priorities:

- in comparison to adults, adolescents view long-term consequences as less important than short-term consequences;
- 'sensation seeking' is a higher priority for adolescents than it is for adults; and
- social status among peers is an important factor for many adolescents.[55]

68.36 Cauffman and Steinberg argue that the big difference between decision making by individuals under the age of 18 and adults is that psychosocial factors can influence the use of cognitive skills by young people during the decision-making process.[56] Three components make up these psychosocial factors:

- *responsibility*, including health autonomy, clarity of identity and self-reliance;
- *perspective*, which is the 'ability to acknowledge the complexity of a situation and see it as part of a broader context'; and
- *temperance*, which is the 'ability to limit impulsive and emotional decision making, to evaluate situations thoroughly before acting … and to avoid decision-making extremes'.[57]

---

52 A Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center—American Bar Association, 2; J Fagan, 'Adolescents, Maturity, and the Law', *The American Prospect* (online), 14 August 2005, <www.prospect.org>.

53 C Wallis and K Dell, 'What Makes Teens Tick', *Time Magazine* (online), 10 May 2004, <www.time.com>, 6.

54 *Inside the Teenage Brain: Introduction* (2002) Public Broadcasting Service <www.pbs.org/wgbh/pages/frontline/shows/teenbrain/etc/synopsis.html> at 10 April 2008.

55 E Cauffman and L Steinberg, 'The Cognitive and Affective Influences on Adolescent Decision-Making' (1995) 68 *Temple Law Review* 1763, 1772–1773.

56 Ibid, 1770.

57 Ibid, 1764.

68.37 This is not to suggest that adolescents are unable to make decisions on their own. The results of the research are consistent, however, with the approach that stresses that an individual's capacity to make a decision cannot be determined by age alone. It also depends on: the maturity of the individual; his or her social development, including his or her relational style with authority and cultural and religious background;[58] and his or her sense of self.[59] Importantly, an individual's capacity to make a decision also depends on the particular decision that needs to be made, its complexity and the gravity of the consequences.[60] This makes an adolescent's maturity of judgment for making a decision highly situation-specific.[61] In the context of making medical decisions, Assistant Professor Leanne Bunney has noted:

> merely because a child may not have the capacity to make decisions in one area does not necessarily imply that he or she would be unable to make decisions in relation to other treatment.[62]

Evolving capacity and the need for individual assessment

68.38 The research suggests, therefore, that the capacity of a child or young person to make a decision is evolving and dependent on a number of considerations relevant to the individual and the particular decision. As discussed above, this understanding of capacity is reflected in art 5 of CROC.

68.39 An individual approach to assessing the capacity of a child or young person has been adopted in case law. The House of Lords decision in *Gillick v West Norfolk and Wisbech AHA* (*Gillick*), and the High Court of Australia decision in *Department of Health and Community Services (NT) v JWB* ('*Re Marion*'), reflect the concept of evolving capacities and the need for individual assessment.[63] In *Re Marion*, Deane J stated that:

> the legal capacity of a young person to make decisions for herself or himself is not susceptible of precise abstract definition. Pending the attainment of full adulthood, legal capacity varies according to the gravity of the particular matter and the maturity and understanding of the particular young person.[64]

---

58 M McCabe, 'Involving Children and Adolescents in Medical Decision Making: Developmental and Clinical Consideration' (1996) 21 *Journal of Paediatric Psychology* 505.

59 L Weiss Roberts, 'Informed Consent and the Capacity for Voluntarism' (2002) 159 *American Journal of Psychiatry* 705.

60 R Ludbrook, 'Children and the Political Process' (1996) 2 *Australian Journal of Human Rights* 278, 376; P Tuohy, 'Children's Consent to Medical Treatment' (2001) *New Zealand Law Journal* 253.

61 E Cauffman and L Steinberg, 'The Cognitive and Affective Influences on Adolescent Decision-Making' (1995) 68 *Temple Law Review* 1763, 1775.

62 L Bunney, 'The Capacity of Competent Minors to Consent to and Refuse Medical Treatment' (1997) 5 *Journal of Law and Medicine* 52, 56.

63 *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112; *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218.

64 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218, 293.

68.40 The words of Deane J, and the individual approach to assessing capacity of a minor, were adopted by the Full Court of the Family Court of Australia in *B and B v Minister for Immigration and Multicultural and Indigenous Affairs*, which considered the capacity of a minor voluntarily to terminate migration detention.[65] Unlike the *Gillick* approach, however, which requires a positive inquiry as to the capacity of a minor to make a particular decision, it has been argued that the Court's approach in *B and B* suggests that capacity is presupposed in some matters, although may be found to be lacking due to certain factors.[66] The Court listed a number of factors, which, in its opinion, may affect the competence of a child. These include 'isolation, English language skills, schooling, access to resources and administrative barriers'.[67] Age was considered to be just one factor to take into consideration. This approach has not as yet been followed in other cases.

Assisting children and young people to make decisions

68.41 In addition to developing decision-making abilities with age, children also develop the capacity to make decisions by being involved in decision-making processes.[68] Dr Mary Ann McCabe argues that 'children's preferences and capacity for involvement in medical decision making will be heavily influenced by their prior experience with taking responsibility in decisions'.[69] McCabe suggests that such experience includes children making different types of decisions in their everyday lives, such as the time they will go to bed.[70]

68.42 Some researchers argue that children have the ability to comprehend difficult concepts that are important for making decisions when the concepts are presented to them in ways that are 'developmentally appropriate'.[71] Nigel Thomas and Claire

---

65 *B and B v Minister for Immigration and Multicultural and Indigenous Affairs* (2003) 199 ALR 604, [373]. The children involved in the case were aged 5, 9, 11, 12 and 14, and were detained with their parents who were appealing the refusal of their claim for refugee status.

66 J Morss, 'But for the Barriers: Significant Extensions to Children's Capacity' (2004) 11 *Psychiatry, Psychology and Law* 319, 319. The High Court of Australia overturned the Full Court of the Family Court's decision concerning its jurisdiction over the welfare of children detained under the *Migration Act 1948* (Cth); however the Full Court of the Family Court's discussion of capacity was not considered by the High Court: see *Minister for Immigration and Multicultural and Indigenous Affairs v B and B* (2004) 219 CLR 365.

67 *B and B v Minister for Immigration and Multicultural and Indigenous Affairs* (2003) 199 ALR 604, [379].

68 M McCabe, 'Involving Children and Adolescents in Medical Decision Making: Developmental and Clinical Consideration' (1996) 21 *Journal of Paediatric Psychology* 505 and R Ludbrook, 'Children and the Political Process' (1996) 2 *Australian Journal of Human Rights* 278.

69 M McCabe, 'Involving Children and Adolescents in Medical Decision Making: Developmental and Clinical Consideration' (1996) 21 *Journal of Paediatric Psychology* 505, 510.

70 Ibid, 510.

71 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 347; N Thomas and C O'Kane, 'Discovering What Children Think: Connections Between Research and Practice' (2000) 30 *British Journal of Social Work* 819.

O'Kane argue that, unless the views of children are sought in ways that enable them to use their competence, children may erroneously be considered incompetent.[72]

Capacity and health information

68.43 The provision of health services to, and the handling of health information about, children and young people is an area that has received more attention than others when considering the decision-making capacity of individuals under the age of 18.

68.44 Consent to the handling of health information about children and young people is related to, but different from, the issue of consent to medical treatment by or on behalf of a child or young person. Although some statutory provisions deal with consent to medical treatment,[73] until the late 20th century the common law assumed that a person under 18 years of age did not have the capacity to make a decision to consent to medical treatment on his or her own behalf. This position has changed. The pivotal case in this area is *Gillick*,[74] which was followed by the High Court of Australia in *Re Marion*.[75]

68.45 These cases affirmed the capacity of 'mature minors' to make their own decisions about medical treatment without parental involvement and reflect the concept of evolving capacities, which is evident in CROC.[76] Neither *Gillick* nor *Re Marion*, however, cover what should be done when a child or young person is assessed as not having capacity to consent to medical treatment, but asks that his or her health information not be disclosed to a parent.[77]

---

72 N Thomas and C O'Kane, 'Discovering What Children Think: Connections Between Research and Practice' (2000) 30 *British Journal of Social Work* 819, 831.

73 See *Minors (Property and Contracts) Act 1970* (NSW) s 49(2), which covers persons aged 14 years and above; *Consent to Medical and Dental Procedures Act 1985* (SA) s 6(1), which covers persons aged 16 years and above. See also New South Wales Law Reform Commission, *Minors' Consent to Medical Treatment*, IP 24 (2004).

74 *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112. This case addressed the issue of whether a minor under the age of 16 years could give consent to contraceptive treatment without the parents' knowledge or consent.

75 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218. This case involved an application before the Family Court of Australia for the sterilisation of an intellectually disabled minor, and addressed the issue of limitations on a parent's right to consent to such treatment. For a discussion of the two cases, see P Parkinson, 'Children's Rights and Doctors' Immunities: The Implications of the High Court's Decision in Re Marion' (1992) 6 *Australian Journal of Family Law* 101.

76 See also United Nations Committee on the Rights of the Child, *General Comment No 4: Adolescent Health and Development in the Context of the Convention of the Rights of the Child* (2003).

77 J Loughrey, 'Medical Information, Confidentiality and a Child's Right to Privacy' (2003) 23 *Legal Studies* 510, 512.

68.46 The ability of young people to keep information from their parents and others is often an important consideration when deciding whether to seek medical treatment. This issue often is discussed as 'confidentiality', but the *Privacy Act* and relevant state and territory health information legislation also regulate the disclosure of health information.

68.47 Young people experience a number of barriers in accessing health services, and lack of confidentiality (or a perceived lack of confidentiality) has been identified as a key problem.[78] In the United States, a study of high school students indicated that a majority of adolescents have health concerns they wish to keep confidential from their parents, and 25% reported that they would not seek health services because of confidentiality concerns.[79]

68.48 When a doctor sees a patient who is a young person without the attendance of a parent or guardian, the doctor must assess the young person's capacity to provide consent to the recommended medical treatment.[80] Factors that will be considered by the doctor include: the maturity of the young person; the capacity to understand and appreciate the proposed procedure and the consequences of the treatment (as well as possible consequences of not receiving treatment); the gravity of the presenting illness and treatment; and family issues.[81] In most cases involving sensitive or serious health concerns, it is suggested that parental involvement be encouraged, and in many cases the involvement of supportive parents may be a key element of successful treatment.[82] It is not always possible or desirable, however, to involve a parent or guardian in this way.

68.49 Similar factors must be taken into consideration by a doctor when deciding whether information can be disclosed to a parent without the consent of the child or young person. The Australian Medical Association (AMA) has stated that, if a young person is able to make autonomous decisions regarding medical treatment and wishes the treatment to remain confidential, his or her doctor must respect and maintain that

---

78 Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004, 21. See also Australian Medical Association, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 22 February 2005, 14; M Booth and others, 'Access to Health Care Among Australian Adolescents: Young People's Perspectives and Their Sociodemographic Distribution' (2004) 34 *Journal of Adolescent Health* 97, 101–103.

79 T Cheng and others, 'Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes Among High School Students' (1993) 269 *Journal of the American Medical Association* 1404.

80 Guidance exists for doctors in dealing with young patients and confidentiality issues. See Medical Practitioners Board of Victoria, *Consent for Treatment of Confidentiality in Young People* (2004); Osteopaths Registration Board of Victoria, *Consent for Treatment of Confidentiality in Young People* (2005); New South Wales Association for Adolescent Health, *Working with Young People: Ethical and Legal Responsibilities for Health Workers* (2005).

81 L Sanci and others, 'Confidential Health Care for Adolescents: Reconciling Clinical Evidence with Family Values' (2005) 183 *Medical Journal of Australia* 410, 411. Family issues may include cultural issues, and also where a parent is unable to act in a protective manner (eg, because of substance abuse or severe mental illness).

82 T Stutt and L Nicholls, *Submission PR 40*, 11 July 2006.

confidentiality.[83] There will, of course, be situations in which the doctor is required to disclose information. Even for adults, there are ethical, statutory and common law exceptions to the duty of confidentiality that require disclosure of information in certain circumstances.[84] Outside of these exceptions, some have argued that confidentiality should be maintained for any young person seeking treatment even if assessed to be incapable of consenting to the appropriate treatment.[85]

68.50 The issue of disclosure of health information to parents sparked public debate in 2003 when the Health Insurance Commission[86] changed its privacy policy to require young people aged 14 and over to give consent before their parents could access their Medicare records.[87] Medicare records include health information such as the identity and speciality of the health service provider, the type of service received, and also may reveal that the individual suffers from certain conditions such as asthma, diabetes, or mental health conditions.[88] The Medicare policy on access to records of an individual under 18 states that:[89]

- if a child or young person of any age has his or her own Medicare card, no information related to the use of the card can be released to a parent or guardian without the consent of the child;[90]

---

83 Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004, 21. See also Australian Medical Association, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 22 February 2005, 15.

84 For example, emergency situations with risk of death or serious injury, reporting of certain infectious diseases, or reporting of risk of harm to a child: L Sanci and others, 'Confidential Health Care for Adolescents: Reconciling Clinical Evidence with Family Values' (2005) 183 *Medical Journal of Australia* 410, 412. For a discussion of disclosure of confidential information in court, see Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Ch 15.

85 See, eg, New South Wales Commission for Children and Young People, *Submission to the New South Wales Law Reform Commission on the Review of Laws Relating to the Consent of Minors to Medical Treatment*, 15 August 2003. See also J Loughrey, 'Medical Information, Confidentiality and a Child's Right to Privacy' (2003) 23 *Legal Studies* 510, 524–525.

86 Now known as Medicare Australia.

87 This policy change, which raised the age from 12 to 14, was based on legal advice: L Sanci and others, 'Confidential Health Care for Adolescents: Reconciling Clinical Evidence with Family Values' (2005) 183 *Medical Journal of Australia* 410. Legal advice to the Australian Government indicated that any further increase of the age would require legislative amendment: T Abbott (Minister for Health and Ageing), 'Parents' Access to Their Children's Medicare Records' (Press Release, 13 November 2003).

88 ABC Radio 891 Adelaide, 'Children's Access to Medicare Cards: Interview with AMA Vice President Dr Mukesh Haikerwal', *Drive with Kevin Naughton*, 6 November 2003.

89 The policy is set out on the Medicare Australia form 'Request for Obtaining Medicare and/or PBS Claims History for a Child'.

90 A young person aged 15 and over can apply for a separate Medicare card without parental approval. A child or young person under the age of 15 can apply for a separate Medicare card with parental approval.

- for a young person aged 14 or 15 on his or her parent's Medicare card, information generally will not be released without the young person's consent, but a parent or guardian may request Medicare Australia to approach any treating medical practitioner to determine if the practitioner will disclose to the parent or legal guardian any information they hold about the young person's treatment; and

- disclosure of information relating to a young person aged 16 and over on his or her parent's Medicare card will be made available to a parent or legal guardian only with the young person's consent.[91]

68.51 Following publication of the changed privacy policy on Medicare records, public debate was split between support for young people's privacy and those concerned that parental rights and family values were being undermined.[92] The Australian Government announced its intention to introduce the Health Legislation Amendment (Parental Access to Information) Bill to raise the age to 16 and over.[93] Following staunch opposition from certain backbenchers, the AMA and others, however, introduction of the Bill was deferred.[94] It has not since been introduced.

68.52 The *Privacy Act* and other Australian health information laws reflect the approach taken by medical practitioners and do not prescribe an age at which a young person is assumed to have the capacity to make decisions on his or her own behalf regarding their personal information.[95] The NPPs dealing with sensitive information (which includes health information) require the capacity of a young person to make decisions relating to disclosure of his or her health information to be assessed on a

---

91 There are limited exceptions to the non-disclosure principle where a young person is under the age of 18 and on the same card as the requesting parent, including access to a Medicare Financial Taxation Statement which shows a total benefit paid for the year but no details of medical services provided, and access to information about the progress of a Medicare claim made by the parent on behalf of the young person.

92 See, eg, Catholic Health Australia, 'CHA Calls for an Informed Public Discussion, Not Political Point Scoring Over Parental Access to Teenagers' Medical Visits' (Press Release, 10 June 2004). The AMA position is that a person aged 15 or over should have the right to keep his or her Medicare records confidential, as at that age people are making independent decisions about their lives, with some leaving school and entering the workforce. The AMA addressed this as a key health issue in the 2004 federal election: Australian Medical Association, 'Youth Health—The Forgotten Area of Health Policy' (Press Release, 9 September 2004); ABC Radio 666 2CN, 'Medicare Under 16 Legislation: Interview with AMA President Dr Bill Glasson', *Morning with Louise Maher*, 15 June 2004.

93 The announcement included funding in the 2004–05 Budget for implementation of the Bill: Australian Government Department of Health and Ageing, *Budget 2004–2005 Health Fact Sheet 5: A Health System Evolving Through Technology* (2004). See also AAP, 'Abbott Backflips on Teen Medical Records', *Sydney Morning Herald* (online), 15 June 2004, <www.smh.com.au>.

94 T Abbott (Minister for Health and Ageing), 'Parental Access Bill' (Press Release, 15 June 2004); P Hudson, 'Backbencher Fears for Teen Lives', *The Age* (online), 13 June 2004, <www.theage.com.au>; D Wroe, 'Abbott Pulls Teen-Health Records Bill', *The Age* (online), 16 June 2004, <www.theage .com.au>.

95 The *Privacy Act 1993* (NZ), *Health Information Privacy Code 1994* (NZ) and *Data Protection Act 1998* (UK) also operate in this way.

case-by-case basis.[96] This may not be possible where there is not a one-on-one personal relationship between the information holder and the individual, and this is reflected in Medicare Australia's age-based policy for disclosure of records of young people. It is noted, however, that Medicare's policy builds in an opportunity for individual assessment of a 14 or 15 year old to be made by a medical practitioner on the request of the parent.

Possible models for assessing capacity

68.53 A number of policy approaches can be taken to the assessment of the capacity of individuals under the age of 18.[97] Capacity could be assessed with reference to the following factors (or a combination of them):

- according to a young person's capacity to understand;
- by fixing a general cut-off age;
- according to the young person's age *and* capacity to understand—for example, by deeming that young people over a certain age have legal capacity, and under a certain age do not have capacity, and for an age bracket in between which would require individual assessment of capacity;
- according to the context of the decision—for example, by setting certain ages of legal capacity in relation to particularly sensitive issues such as access to information relating to a termination of pregnancy, or disclosure to the family of a missing young person's location; or
- according to specific groups of young people—for example, by deeming young people who are married, parents themselves, living independently or homeless to have legal capacity.

68.54 Research on the decision-making capacity of children and young people, international law as reflected in CROC, and recent case law all support an individual assessment of capacity. This approach is consistent with the existing regime understood and applied under the *Privacy Act*, and in other privacy legislation in Australia. There also is strong support in the community for continuing this approach. Further, a model that involves communicating with a child or young person to help him

---

96 See also Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001).

97 These approaches are based on models developed by the New South Wales Law Reform Commission in considering the consent of minors to medical treatment: New South Wales Law Reform Commission, *Minors' Consent to Medical Treatment*, IP 24 (2004), Ch 3. The NSWLRC is expected to complete its report on this project in 2008.

or her to understand the nature and consequences of a decision is the best model for involving children and young people in decision-making processes, even where the child or young person is found to be incapable of making the decision without assistance. The assessment process lends itself to involving parents, guardians or other supporting adults, so that the child or young person receives support whether he or she is capable or incapable of making an independent decision.

68.55 There are practical limitations and difficulties with this approach. Individual assessment presupposes that it is possible to engage with the individual. It also requires that the person making the assessment is suitably qualified to provide support and make an appropriate judgment about the capacity of the individual to understand the nature and consequences of the decision. While such a situation generally exists in a doctor-patient relationship, it does not exist in a wide variety of circumstances involving decisions regarding an individual's personal information. Such circumstances include an individual:

- completing an online form with personal information in order to access subscriber-only parts of a website, where the conditions of access (set out on the website) include allowing the company to use the personal information for marketing purposes;

- providing staff at a gym with a form containing details of medical conditions;

- agreeing over the phone to participate in a survey, and disclosing sensitive personal information during the phone interview;

- completing a form in which he or she agrees to the use by an organisation of his or her personal information held by the organisation for research purposes; or

- sending a letter or email to an agency, or completing an online form, requesting access to a record containing his or her personal information.

68.56 In many of these situations, the agency or organisation may not be aware of the age of the individual it is engaging with, let alone be able to make an assessment regarding the capacity of the individual to understand the nature and consequences of the decision. While the individual in each scenario may appear to consent to the collection or disclosure of, or access to, his or her personal information, the agency or organisation does not know whether the individual understands fully the consequences that may arise from the decision. At present, in the absence of making a one-on-one assessment concerning the capacity of an individual under the age of 18, the *Privacy Act* provides no guidance on how to handle personal information in such situations.

68.57 Setting a minimum age at which individuals are assumed to be able to make decisions under the *Privacy Act* would clarify the operation of the law and simplify processes for determining capacity. So long as an agency or organisation can establish

that an individual is of the age where he or she is presumed to have capacity, no assessment of capacity would be required.[98]

68.58 Setting a minimum age also would have the benefit of protecting those under that age, by requiring a person with parental responsibility to make decisions on their behalf.[99] This would be appropriate where there are serious or possibly negative consequences of a decision regarding personal information, and the child or young person is not capable of giving appropriate consideration to those consequences. A person with parental responsibility would be required to make, or refuse to make, the decision on behalf of the child or young person, and ensure the child or young person is supported in all the circumstances.

68.59 The simplicity of the minimum age solution, however, also has the potential to cause injustice. It has been suggested that the application of any age-based legislative provision is arbitrary, and may breach the principle of equality before the law.[100] It is inevitable that, at whatever age the barrier is placed, there will be some over the age that do not have the required capacity, and there will be some under the age that would have the required capacity.

68.60 If a specified age option is desirable, the next step is to determine the appropriate age. Research on child development and brain development suggests that the cognitive ability to make independent decisions is generally in place by the age of 14 to 16, but this cognitive ability has not fully matured and individuals of this age will continue to be more susceptible than adults to psychosocial factors. The impact of psychosocial factors will differ depending on the circumstances in which the decision must be made and the potential consequences of the decision. Also relevant are the circumstances of the individual, including his or her stage of social development, socio-economic status, and the support available to, and accepted by, the individual.

68.61 It may be appropriate to make the age of presumption dependent on the nature of the personal information involved. For example, decisions regarding health information may involve more complex considerations, and attract more significant consequences, than decisions regarding disclosure of an email address for direct marketing purposes.[101] The *Privacy Act* already makes a distinction between sensitive information and other personal information and applies additional protection to

---

98 The agency or organisation would need to be alert to issues concerning capacity generally, as in relation to its dealings with all adult individuals: see Ch 69.

99 The term 'authorised representative', and who may be an authorised representative, are discussed further below.

100 J Morss, 'But for the Barriers: Significant Extensions to Children's Capacity' (2004) 11 *Psychiatry, Psychology and Law* 319, 321–322.

101 It should be noted that the consequences of access to, and disclosure of, health information may differ from decisions regarding health treatment. This is discussed below.

sensitive information.[102] It may be appropriate to set a higher minimum age for making decisions relating to sensitive information than to other personal information. While this approach is likely to cause some confusion for agencies, organisations and individuals, the fact that differing requirements already apply to the handling of sensitive information suggests it is possible to implement this approach.

68.62 Consideration could also be given to a deeming provision for certain categories of young people. For example, those who, in practice, act independently of their parents or guardians could be deemed to possess legal capacity for the purposes of decisions made under the *Privacy Act*. Any situation requiring such individuals to have a person with parental responsibility to make a decision on their behalf may be impractical. It would be possible to include such an approach under the *Privacy Act*, although it may not be easy to define the categories and it would require additional administrative steps to prove a certain individual falls within a particular category.

Models used in other jurisdictions

68.63 Most privacy legislation overseas takes the same approach as Australian privacy legislation in assuming all individuals, regardless of age, have the same level of protection for their personal information. Some overseas legislation makes provision, however, for determining when a child or young person may make decisions in his or her own right, or for determining who may make decisions on behalf of the child or young person.

68.64 The *Privacy Act 1985* (Canada) and the *Personal Information Protection and Electronic Documents Act 2000* (Canada) provide that rights or actions may be exercised or performed on behalf of a minor by an authorised person. It is assumed that an individual assessment approach is used in practice, although there is no guidance on the issue.

68.65 The United Kingdom uses a combined individual assessment and minimum age approach. Guidance has specified that an individual aged 12 or more is presumed to be of sufficient age and maturity to have the required understanding to exercise a right under the *Data Protection Act 1998* (UK), but that an assessment of capacity should be made.[103]

---

102 The ALRC proposes retaining this distinction for sensitive information. For the definition of sensitive information, see Ch 6. See Ch 22 for a discussion of the provisions relating to sensitive information in the model UPPs.

103 This position is set out in the Act only in relation to Scotland, which otherwise deems that an individual does not have legal capacity until the age of 16: *Data Protection Act 1998* (UK) s 66. This also means that in Scotland an individual aged 16 has legal capacity, and no assessment is required. It was not considered necessary to spell out this position in the legislation in relation to Wales, England and Northern Ireland: United Kingdom Government Information Commissioner's Office, *Data Protection Act 1998 Legal Guidance* (2001), 52.

68.66 The *Privacy Act 1993* (NZ) also uses a combined individual assessment and minimum age approach. The Act gives an agency the power to refuse to disclose information requested by an individual under the age of 16 if the disclosure would be contrary to the individual's interests.[104] There is no further guidance in the legislation or otherwise about assessing the capacity of a child or young person to make decisions under the Act, although an individual assessment approach can be assumed. The exception is in the *Health Information Privacy Code 1994* (NZ), issued under the *Privacy Act*, which provides that, where an individual is under the age of 16, the individual's parent or guardian may make decisions regarding the collection, use and disclosure of health information.[105] As the provision is permissive, it does not preclude a child or young person from making a decision in his or her own right, but suggests that a decision by a parent or guardian will take precedence over that of the individual under the age of 16.

68.67 The *Personal Health Information Protection Act 2004* (Ontario) has a number of interesting provisions relating to capacity, which combine an individual assessment and minimum age approach. Essentially, it assumes that a person aged 16 or over can consent to the collection, use or disclosure of personal information in his or her own right. It goes on to provide that a parent, children's aid society or other person with parental responsibility may provide consent on behalf of an individual who is under the age of 16, but not if the information relates to: medical treatment about which the individual has made his or her own decision; or child and family services counselling in which the individual has participated on his or her own.[106] The provision that parents or others may provide consent on behalf of an individual under the age of 16 is further qualified, however: if the individual is considered to be capable of consenting on his or her own, then the decision of the individual prevails over a conflicting decision of the parent or other substitute decision-maker.[107]

Approach to reform

68.68 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC determined that there was a need to clarify the *Privacy Act's* approach to decision making by individuals under the age of 18. The ALRC proposed that a model be incorporated into the Act that required individual assessment of capacity when practicable, but a legislative presumption of capacity at age 15 or over where assessment is not practicable.[108] The approach to individual assessment of capacity

---

104 *Privacy Act 1993* (NZ) s 29(1)(d). This also means that there is no power to refuse if the individual is aged 16 or over.

105 *Health Information Privacy Code 1994* (NZ) cl 3.

106 *Health Information Protection Act 2004* (Ontario) s 23(2). Each of these exceptions applies to sensitive areas that are regulated by other legislation dealing with the capacity of the individual to provide consent or participate in his or her own right, namely the *Health Care Consent Act 1996* (Ontario) and the *Child and Family Services Act 1990* (Ontario).

107 Ibid s 23(3).

108 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007) Proposal 60–1.

reflected the existing law. The ALRC acknowledged, however, that in many situations an agency or organisation would not be able to make an individual assessment—either because the method of interaction (eg, online) precluded individual assessment or the staff of an agency or organisation were not sufficiently trained to make such an assessment. The age of 15 was selected following consideration of the research on adolescent decision making and the types of decisions made under the *Privacy Act* and likely consequences of those decisions. It was also consistent with the age at which a young person is entitled to access a separate Medicare card without parental permission.

Submissions and consultations

68.69 There was general support from stakeholders for the inclusion of provisions in the *Privacy Act* clarifying the handling of personal information of children and young people.[109] There were opposing opinions, however, on whether the ALRC's proposals were appropriate.

68.70 A number of stakeholders highlighted particular areas where they considered it important for young people to be able to participate without the need to disclose information to parents. Access to health services was one such area mentioned.[110] Accessing library services also was raised as a concern.[111]

68.71 A number of stakeholders indicated that parents and guardians should continue to have full access to personal information relating to their children until the child reaches 18 years of age, and that this approach should be incorporated expressly into the *Privacy Act*.[112] Stakeholders expressing this view were concerned about the decision-making capacity of individuals under the age of 18, and maintained that parents and guardians are the best people to make decisions in the best interests of the child or young person. The Festival of Light Australia acknowledged that, while the capacity of minors to make their own decisions develops with age, parents are best

---

109 See, eg, Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171*, 5 February 2007; K Pospisek, *Submission PR 104*, 15 January 2007.

110 Australian Medical Association, *Submission PR 524*, 21 December 2007; New South Wales Aboriginal Justice Advisory Council, *Submission PR 501*, 20 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 172*, 5 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; National Children's and Youth Law Centre, *Submission PR 166*, 1 February 2007; Council of Social Service of New South Wales, *Submission PR 115*, 15 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007

111 N Bradley, *Submission PR 573*, 22 February 2008.

112 BUPA Australia Health, *Submission PR 455*, 7 December 2007; Festival of Light Australia, *Submission PR 354*, 1 December 2007; Confidential, *Submission PR 340*, 4 November 2007; D Bowman, *Submission PR 330*, 19 October 2007; R Sands, *Submission PR 317*, 12 September 2007.

equipped to make a thorough assessment of the child's capacity to make a particular decision.[113]

68.72 The Caroline Chisholm Centre for Health Ethics expressed a contrary view.

> In familial settings there are wide ranging situations where it could be argued that the parent abdicates certain rights that accompany parental responsibility because of neglect, emotional, psychological and physical abuse, or their own drug use, or other harmful behaviour which negatively impacts on the child … It is therefore not possible to argue that it is always in the child's best interest for the parent to be able to access the health information of the child, where the child has independently sought medical, welfare or social services care, and because of fear or parental reaction, has decided to conceal this information from the parental figure(s).[114]

68.73 One individual suggested that parents should not always be seen as 'baddies' from whom young people need to be protected.[115] The New South Wales Commissioner for Children and Young People also emphasised that children and young people do not necessarily exclude parents from decision-making processes even as they increase their own involvement.

> Many children and young people tell the Commission that they want their parents to be involved in their lives and to assist them when needed and so want to share their personal information with their parents. However, as young people grow older and seek assistance with more intimate issues they want to choose if and when their parents are involved. Therefore, laws on how information is collected and disclosed need to reflect this need for flexibility.[116]

68.74 A number of stakeholders opposed any attempt to clarify issues of capacity and regulate decision making by individuals under the age of 18.[117] These stakeholders highlighted the problems for agencies and organisations that regularly deal with children and young people in making assessments regarding capacity or otherwise obtaining consent from parents of individuals under a specified age. It was suggested the proposals would be 'a detriment to young people' by depriving them of opportunities to participate in activities such as birthday clubs and competitions where personal information is collected for marketing purposes.[118]

---

113 Festival of Light Australia, *Submission PR 354*, 1 December 2007.

114 Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006. See also New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007; and L Mitchell, *Submission PR 46*, 2 June 2006 in relation to children and young people living apart from parents because of a conflict.

115 A Hugo, *Submission PR 285*, 19 April 2007.

116 NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007.

117 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007.

118 Law Council of Australia, *Submission PR 527*, 21 December 2007.

68.75 The National Catholic Education Commission (NCEC) and the Independent Schools Council of Australia (ISCA) also opposed the proposals for individual assessment or an age-based presumption. Instead, they preferred to retain flexibility within the school environment without having decision making hampered by 'artificial and irrelevant considerations'. They indicated that schools must balance a variety of complex factors and must make decisions that, in each situation, reflect the best interests of the child involved.

> The schools are very concerned that the proposals fail to appreciate the practical situations that arise in schools on a daily basis and, if implemented, will distort the decision-making process which school staff need to employ in the course of their duties.[119]

68.76 Three stakeholders supported the retention of the individual assessment approach in all circumstances and rejected the ALRC's proposal for an age-based presumption in the absence of a practicable opportunity for assessment.[120] SBS opposed the proposal on two grounds. First, it argued that the journalist's assessment of the capacity of a child or young person participating in an interview or discussion should be paramount. Secondly, it was concerned about preventing individuals under the age of 15 from participating in online activities such as competitions, discussions and educational initiatives.[121]

68.77 A number of stakeholders suggested that the age at which capacity is assumed should be reduced from 18 to a lower age, with no assessment required from the age of 16[122] or, in relation to health information, 15.[123]

68.78 The majority of stakeholders that addressed these issues, however, supported the ALRC's approach to reform.[124] One agency indicated that a set age would ensure consistency of application across the various jurisdictions involving interaction with children and young people.[125] A number of stakeholders acknowledged the need for the age-based presumption, although wanted further emphasis on the requirement to undertake an assessment.[126] There were concerns that the age-based presumption

---

119 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

120 Special Broadcasting Service, *Submission PR 530*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

121 Special Broadcasting Service, *Submission PR 530*, 21 December 2007.

122 Confidential, *Submission PR 519*, 21 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

123 Privacy NSW, *Submission PR 468*, 14 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

124 Including the following stakeholders who did not provide any detailed comment on the proposals: Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.

125 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

126 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*,

would be used by many agencies and organisations without consideration of the need to undertake an assessment. The ALRC's proposal to undertake assessment used the words 'where practicable', but stronger language was urged by some stakeholders, including the terms 'take all reasonable steps',[127] 'take all steps possible',[128] or 'where at all possible'.[129]

68.79 The OPC suggested that the following factors may help to decide whether or not it is 'reasonable and practicable' to undertake an assessment:

- the type of personal information in question;
- the proposed handling of that information;
- the degree to which appropriately skilled staff are able to conduct the assessment; and
- how young the child is (eg, it is likely to be unreasonable to conduct an assessment of a 7 year old).[130]

68.80 Other stakeholders gave strong support to the age-based presumption, highlighting the impracticality of individual assessment in many environments.[131] There were, however, differences of opinion as to the most appropriate place to set the age-based presumption. Some argued for a lowering of the age to 13, making it consistent with regulation of the online environment in the United States.[132] Others argued that the ALRC had misinterpreted the research and set the age presumption too low.[133] In youth workshops conducted by the ALRC, there were varying suggestions about the age at which most young people should be able to control access to their personal information, although it was generally placed around the age of 14 to 16.[134]

---

20 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Tasmanian Government Department of Health and Human Services, *Submission PR 436*, 10 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007.

127 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

128 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

129 Youthlaw, *Submission PR 390*, 6 December 2007.

130 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

131 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007; Australian Health Insurance Association, *Submission PR 161*, 31 January 2007.

132 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; ASTRA, *Submission PR 426*, 7 December 2007.

133 BUPA Australia Health, *Submission PR 455*, 7 December 2007; Festival of Light Australia, *Submission PR 354*, 1 December 2007.

134 See discussion on youth workshops in Ch 67.

68.81 A number of stakeholders agreed with the ALRC's proposal that the age-based presumption of capacity be set at 15 years of age, with the Privacy Foundation of Australia noting that this reflects an 'appropriate balance between the autonomous capacity of 15+ year olds and at the same time providing protection for younger children'.[135]

68.82 A number of stakeholders pointed out the problems with setting an age when other legislation sets alternative ages of capacity, including:

- the *Motor Accidents Compensation Act 1999* (NSW) which sets the age of consent at 18 years for making decisions or executing documentation in relation to personal injury claims;[136]
- the *Minors (Property and Contracts) Act 1970* (NSW) which effectively requires parental consent to medical treatment for an individual under the age of 14;[137]
- obligations on parents to provide the necessities of life, including medical attention, to children under the age of 16;[138] and
- banking relationships based on contract law that allows a minor to open a bank account but not to authorise another person to operate the account.[139]

68.83 Other stakeholders suggested additional provisions to qualify or add to the ALRC's proposals, including:

- a requirement that consideration be given to the best interests of the child when handling personal information relating to all children under the age of 18;[140]
- that the views of a child or young person should be heard and considered as part of the decision-making process, even where a child or young person is found to be incapable of making his or her own decision;[141] and

---

135 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also support from Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Obesity Policy Coalition, *Submission PR 506*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

136 Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

137 Australian Medical Association, *Submission PR 524*, 21 December 2007.

138 Festival of Light Australia, *Submission PR 354*, 1 December 2007.

139 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

140 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007. See also National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

141 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

- a stipulation in the *Privacy Act* that, where health information has no short-term impact on the circumstances of an individual under the age of 18, clinical decision making cannot be the sole responsibility of the patient.[142]

68.84 The AMA was concerned that different age limits for the regulation of consent to disclosure of personal information would 'muddy' the regulation of consent to medical treatment.[143] It was stressed by some stakeholders, however, that the assessment of an individual's capacity to consent to medical treatment differs from a decision to disclose personal information. The individual may be unable to consent to the medical treatment (particularly where it is of an invasive nature or has serious consequences), but have the capacity to determine that the practitioner should not disclose the fact and details of the treatment.[144]

68.85 The distinction between consent to medical treatment and the disclosure of personal information will become more important if Australia moves to a national electronic health record system. Such a system may involve decisions to opt in or opt out of the system, or stipulate who should have access to the record.

> The requirement of health practitioners to assess the capacity of a young person to consent to an electronic health record has raised particular concerns. Assessing a young person's capacity to make decisions about the handling of their personal and health information … is different to assessing a young person's capacity to make decisions about their healthcare or medical treatment. Therefore is the use of 'standard clinical practice' appropriate? The distinction between capacity to make decisions about privacy, and capacity to make decisions about healthcare needs to be more clearly articulated in any electronic health record implementation.[145]

Assessing capacity

68.86 In DP 72, the ALRC proposed that the *Privacy Act* be amended to incorporate a test of capacity to be applied when assessing an individual under the age of 18.[146] The proposal indicated that individuals under the age of 18 who are found to be incapable of making a decision—either because of an individual assessment or application of the

---

142 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007. These organisations were concerned about the implications of giving young people 'control' of their health information and making requests for genetic tests.

143 Australian Medical Association, *Submission PR 524*, 21 December 2007.

144 Youth Affairs Council of Victoria Inc, *Submission PR 172*, 5 February 2007; Council of Social Service of New South Wales, *Submission PR 115*, 15 January 2007.

145 Council of Social Service of New South Wales, *Submission PR 115*, 15 January 2007.

146 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 60–2. The same test of capacity was proposed in relation to adults (Proposal 61–1), although with the concept of 'maturity' added to the list of factors that may affect the capacity of an individual under the age of 18.

age presumption—must have an authorised representative make the decision on their behalf. The proposal also clarifies who has responsibility in such situations.[147]

68.87 A number of stakeholders supported the inclusion of the test of capacity in the *Privacy Act*.[148] A number of suggestions were made to simplify the wording of the test, in particular removing the list of specific factors that may give rise to incapacity (such as maturity, injury, disease, illness, cognitive impairment, physical impairment, mental disorder or any disability) and focusing instead on the general nature and effect of giving the consent, and the individual's capacity to communicate consent.[149] The OPC had concerns about adding the term 'any other circumstance' to the end of the list of specific factors, considering it too broad.[150]

68.88 In contrast, two stakeholders considered that it was not necessary to set out a test of capacity in the *Privacy Act*.[151] They argued that OPC guidance was more appropriate.

68.89 Stakeholders generally did not comment on the proposal to specify in the *Privacy Act* the authority of persons with parental responsibility to make decisions on behalf of a child or young person who is considered to be incapable of making such decisions. The Obesity Policy Coalition, however, gave strong support for the requirement that a parent or other person make decisions on behalf of a child under a set age.[152]

Verifying age

68.90 In DP 72, it was noted that agencies and organisations that deal with children and young people may have to establish a system for either assessing capacity or verifying the age of individuals. If individuals are under the age of 15, agencies and organisations will have to establish alternative methods for communicating directly with an authorised representative. The ALRC did not suggest including specific requirements for age verification processes in legislation, but considered that guidance should be developed by the OPC to assist agencies and organisation to establish appropriate mechanisms and practices for implementing the age of presumption. Such

---

147 The definition of 'authorised representative' included, for individuals under the age of 18, a person with parental responsibility for the individual: see Ibid, Proposal 61–2.

148 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

149 Youthlaw, *Submission PR 390*, 6 December 2007 who consulted with the Youth Disability Advocacy Service on this proposal; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

150 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

151 Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007. Privacy NSW advocated that the matters be set out in binding guidelines issued by the OPC.

152 Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.

mechanisms would include establishing appropriate age verification mechanisms and facilitating decision making by authorised representatives on behalf of children and young people lacking capacity.[153] The ALRC proposed that the *Privacy Act* provide that an agency or organisation will not be considered to have acted without consent if it did not know, or could not reasonably be expected to have known from the information available, that an individual was aged 14 or under, and the agency or organisation acted upon the consent given by the individual.[154]

68.91 There was strong support from stakeholders for a limitation on the liability of agencies and organisations when relying on the age-based presumption.[155] There were, however, different opinions on the wording to be included in the provision and the extent of the onus on agencies and organisations to verify the age of the individual.

68.92 A number of stakeholders considered it to be appropriate to place the onus on the individual to provide correct and timely information to the agency or organisation, and not hold the agency or organisation responsible where the age has been falsified.[156] Others considered that the wording was too open to abuse. A number of stakeholders suggested that agencies and organisations should be required to take 'reasonable steps' to verify the age of the individual.[157] The OPC suggested that 'due diligence' should be exercised.[158] The Law Society of New South Wales considered that agencies and organisations should be required to 'explore' the circumstances to ascertain whether the information is correct.[159]

68.93 A number of submissions focused on the practical limitations of establishing age verification mechanisms. The Law Council of Australia noted the practical problems that have been encountered in determining an appropriate 'Restricted Access System' and age verification mechanism to prevent young people from accessing MA15+

---

153 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [60.106].

154 Ibid, Proposal 60–4.

155 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Obesity Policy Coalition, *Submission PR 506*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; ASTRA, *Submission PR 426*, 7 December 2007.

156 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; ASTRA, *Submission PR 426*, 7 December 2007.

157 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007. Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007 indicated that 'all reasonable steps' should be taken. The Obesity Policy Coalition suggested that reasonable steps must be taken, and it must be reasonable in the circumstances to rely on the information: Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.

158 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

159 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

content on the internet and via mobile phones.[160] The Australian Direct Marketing Association indicated that it is 'extremely difficult and onerous for businesses to accurately ascertain the age of both current and prospective customers'.[161]

68.94 The Obesity Policy Coalition also noted the limitations of existing age verification mechanisms.

> Introduction of the age of presumption would have little effect if an organisation could escape liability by taking cursory steps to ascertain a young person's age or seek an authorised representative's consent, such as asking the young people to provide their dates of birth, and, if they admit to being younger than 15, asking them to indicate (e.g by ticking a box) that an authorised representative consents to the proposed use of their personal information. Some organisations currently use these types of practices when collecting children's personal information for direct marketing through competitions, website registrations and so on. For example, to register for the competitions and promotions section of the Cadbury website, people must agree to use of their personal information for direct marketing and enter their age range (<16, 16–17 or 18+). The registration page states that 'Children under 16 are advised to get permission from their parent or guardian before they submit any personal information to Cadbury.' In situations like this, many children would be likely to lie about their age or the fact that their parent has consented, or ignore advice to seek parental consent, if this would allow them to immediately enter a website or participate in a desired activity.[162]

68.95 The OPC was concerned that a lack of robust age verification mechanisms would make the ALRC's proposals problematic.[163] Microsoft Asia Pacific also noted the significant limitations associated with existing age verification technologies, but submitted that it expects market-driven solutions to be forthcoming in the near future.[164]

68.96 ASTRA submitted that it should be sufficient for organisations to establish reasonable age verification procedures, and they should not be subject to onerous rules. It stated that tighter restrictions would be appropriate for those organisations handling particularly sensitive information.[165] Microsoft indicated its support for the ALRC's proposal that guidance on these issues be provided by the OPC rather than through prescriptive legislative provisions.[166] In contrast, the Obesity Policy Coalition was concerned that dealing with age verification procedures in guidance, rather than by establishing enforceable legal requirements, would result in non-compliance.[167]

---

160 Law Council of Australia, *Submission PR 527*, 21 December 2007. The regulatory structure for the implementation of the *Communications Legislation Amendment (Content Services) Act 2007* (Cth) has been developed by the Australian Communications and Media Authority: see Restricted Access Systems Declaration 2007 (Cth).

161 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

162 Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.

163 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

164 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

165 ASTRA, *Submission PR 426*, 7 December 2007.

166 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

167 Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.

Implementing the provisions

68.97 To facilitate implementation of the new provisions dealing with decision making by individuals under the age of 18, the ALRC proposed:

- the development of guidance by the OPC, which should focus on applying the provisions in practice;[168] and

- a requirement on agencies and organisations that handle the personal information of individuals under the age of 18 to address in their Privacy Policies how such information is managed and to ensure staff are adequately trained to assess the decision-making capacity of children and young people.[169]

68.98 All but one stakeholder that addressed the issue gave support for the development of guidance by the OPC.[170] Similarly, there was strong support for including in Privacy Policies relevant information on the handling of personal information of individuals under the age of 18.[171]

68.99 There also was support for the ALRC's proposal on staff training.[172] The National Children's and Youth Law Centre submitted that:

> The development of the knowledge and skills to recognise and respect the rights of all children to privacy, to explain the processes and decisions in age-appropriate language, to make assessments of decision-making capacity and, regardless of the

---

168 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 60–4.

169 Ibid, Proposals 60–5, 60–6.

170 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007.

171 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

172 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007.

> results of such assessments, to engage children in the decision-making processes to the fullest extent of their capacity are important goals.[173]

68.100 There was, however, opposition to the training requirements. The Australian Bankers' Association indicated:

> An obligation for banks to train staff to undertake assessments of the capacity of minors is onerous, costly and potentially of disadvantage to minors in introducing a complex process over the top of long standing simple practices of opening and maintaining accounts for minors, eg school bank accounts.[174]

68.101 A number of other stakeholders considered that the requirement to train staff to undertake assessment of the decision-making capacity of those under the age of 18 was unreasonable, impracticable and inappropriate, and had significant compliance costs.[175] The Australian Taxation Office considered that the training requirement should be confined to those bodies whose functions specifically include service provision to client groups including individuals under the age of 18.[176]

ALRC's view

Combining individual assessment and age of presumption approaches

68.102 A system of individual assessment is the fairest and most appropriate way to determine if an individual under the age of 18 has the capacity to make a decision. As far as possible, a system of individual assessment should be incorporated formally into the *Privacy Act*.

68.103 The ALRC is alert, however, to the impracticalities of imposing an 'across-the-board' individual assessment approach. Decisions relating to personal information arise in a wide variety of contexts, many of which do not allow for individual assessment by the relevant agency or organisation. At present, it is assumed that an individual who completes a form, makes a phone call or ticks a box has the capacity to make the required decision regarding his or her personal information. The consequences of the decision to allow collection or disclosure of personal information, however, can be significant. This is of particular concern given that children and young people increasingly interact with agencies and organisations in the online environment without adult supervision.

68.104 The ALRC recommends a model that combines individual assessment and a minimum age of presumption of capacity. In all circumstances where an individual assessment is reasonable and practicable, any individual under the age of 18 should be

---

173 National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.

174 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

175 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Medical Association, *Submission PR 524*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007.

176 Australian Taxation Office, *Submission PR 515*, 21 December 2007.

assessed to determine if he or she has the capacity to make a decision to give consent, make a request or exercise a right of access under the Act. Where individual assessment is not reasonable or practicable, there should be a set age at which a presumption of legal capacity exists, and under which it is presumed the individual cannot make a decision in his or her own right. Even if a presumption is initially adopted, the presumption subsequently may be overridden by an individual assessment.

68.105 This approach has two benefits. First, the individual assessment element is flexible and recognises the ways in which cognitive capacity develops. Second, it provides certainty and enables practical operation in those situations where individual assessment is not reasonable or practicable.

68.106 The ALRC is aware that setting an age of presumption in the legislation may have a negative effect on the system of individual assessment and, in practice, suggest a general presumption for all decisions regarding personal information. The age of presumption is intended to be a fall back position, only to be relied upon in certain circumstances.

68.107 In DP 72, the ALRC used the words 'where it is practicable' to define when an individual assessment should be undertaken. The ALRC is now of the view that an individual assessment should be undertaken where it is 'reasonable and practicable'. This obligation is consistent with a number of the model UPPs that seek to establish high-level obligations on agencies and organisations to undertake certain activities, while acknowledging cost compliance issues and practical business requirements.[177]

Setting the age of presumption

68.108 As outlined above, in many jurisdictions the age of presumption of legal capacity in relation to privacy decisions has been set at 16, with individual assessment below that age that allows for recognition of capacity in individual circumstances. In the United Kingdom it is assumed that those under the age of 12 do not have capacity, but legislation provides for individual assessment to be conducted above that age. COPPA in the United States, which is focused on the protection of children's privacy in the online environment, requires parental authority or consent before personal information can be collected from any child under the age of 13.[178]

68.109 If the ALRC's recommendations are implemented, the age of presumption of capacity will apply only where individual assessment is not reasonable or practicable.

---

177 See the 'Collection', 'Direct Marketing' and 'Access and Correction' principles.

178 See, eg, *Children's Online Privacy Protection Act 1998* 15 USCA § 6501 (US). This influenced the Australian Labor Party's proposed amendment to the *Privacy Amendment (Private Sector) Act 2000* (Cth) headed 'Special protection for children' also adopted this cut-off age: Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2006, 20302 (N Bolkus). See also Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001).

The age chosen must provide appropriate recognition of the capacity of the vast majority of individuals above a certain age, without exposing a large number of individuals to the potential consequences of decision making they are not equipped to deal with.

68.110 The balance between parental authority and the evolving capacities of young people to make decisions on their own also must be considered. The recognition of legal capacity will allow young people above a certain age to refuse to consent to disclosure of personal information to others, including their parents.[179]

68.111 While many global corporations are familiar with COPPA and already have policies and practices in place on their websites to facilitate parental consent requirements for individuals aged 12 or under, the ALRC does not consider that 13 is an appropriate age at which to expect all young people to take on the responsibilities and consequences of decision making relating to personal information.

68.112 Given previous debates in the Australian community, and the latest research that highlights the impact of psychosocial factors on adolescent decision making, the ALRC recommends that the minimum age for presumption of capacity be set at 15. Fifteen is the age at which a young person is entitled to obtain a separate Medicare card without parental permission. Under the ALRC's recommendation, where an individual assessment is not reasonable or practicable, individuals aged 15 and over will be assumed to have the capacity to make decisions under the *Privacy Act*. Individuals under the age of 15 must have a person with parental responsibility make the decision on their behalf.

Assessing capacity

68.113 In DP 72, the ALRC proposed that a test of capacity be included in the *Privacy Act*. The test of capacity was intended to be applied when assessing the capacity of adults, as well as individuals under the age of 18. In Chapter 70, the policy basis for setting out a test of capacity in the *Privacy Act* is discussed. The ALRC concludes that it is not appropriate to set out a particular test for capacity in the *Privacy Act*. Sufficient clarification can be given in guidance to be developed and published by the OPC, drawing on existing literature regarding the assessment.[180]

Making decisions for a child or young person who lacks capacity

68.114 The *Privacy Act* does not provide any mechanism for making decisions on behalf of an individual under the age of 18 who is found, either by assessment or a reliance on the presumption, to be incapable of making a decision on his or her own behalf. It is assumed that parents or guardians will make these decisions. In DP 72, the

---

179 The disclosure will be permissible if this is expected as part of the primary purpose of collection, or a related secondary purpose. See, eg, the discussion on this point in relation to school reports in Ch 69.

180 See Rec 68–4 below for guidance on these issues to be developed by the OPC.

ALRC proposed that the position be clarified in the *Privacy Act* and suggested specifying that a person with 'parental responsibility' must make such decisions.[181] The term 'parental responsibility' has been adopted in many Australian statutes dealing with duties, powers, responsibilities and authority of parents and persons acting as parents.[182]

68.115 This issue did not elicit many comments from stakeholders, although the ALRC notes general support for the clarification of the requirements for the handling of personal information of children and young people.

68.116 It is necessary to give specific legislative authority to persons with parental responsibility to make these kinds of decisions on behalf of children and young people lacking capacity. The duty of parents to provide for the welfare of their children implicitly gives authority to parents to make a range of decisions on behalf of their children who lack capacity,[183] but unlike other particular areas of decision making, there is no case law on matters relating to the handling of personal information.[184] It is not unusual for legislation to provide specific authority to persons with parental responsibility to make decisions on behalf of children and young people, including privacy legislation in a number of Australian and overseas jurisdictions.[185] Some Australian case law has interpreted the lack of specific legislative authority as showing a deliberate intention to omit parental authority.[186]

68.117 The term 'person with parental responsibility' encompasses parents, guardians, foster carers and other persons given parental responsibility by statute or a court order. The common law doctrine of *in loco parentis* also will operate to enable other persons standing in the role of parent either on a permanent or temporary basis—such as teachers, adult siblings, grandparents and carers—to make decisions on behalf of a child or young person lacking capacity. The authority for those other persons to

---

181 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [60.101], Proposals 60–2, 61–2.

182 See, eg, *Family Law Act 1975* (Cth) s 61B; *Children and Young Persons (Care and Protection) Act 1998* (NSW) s 3; *Adoption Act 1994* (WA) s 4.

183 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218, 278, 315–317; *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112.

184 For a list of the kinds of decision making authorities that have been considered by the courts, see J Seymour, 'An "Uncontrollable" Child: A Case Study in Children's and Parents' Rights' in P Alston, S Parker and J Seymour (eds), *Children, Rights and the Law* (1992) 98, 113.

185 See, eg, *Health Records and Information Privacy Act 2002* (NSW) s 7; *Health Records Act 2001* (Vic) s 85(6); *Health Records (Privacy and Access) Act 1997* (ACT) s 25; *Health Information Privacy Code 1994* (NZ) cl 3; *Health Information Protection Act 2004* (Ontario) s 23(2).

186 *Hinch and Television and Telecasters (Melbourne) Pty Ltd* (1996) 85 A Crim R 555. The legislation under consideration allowed the disclosure of the identity of a victim of sexual assault with the consent of the victim or the court. In this case, the victim was an eight year old boy and his parents had consented to the disclosure of the boy's identity. The court ruled that the child did not have capacity to consent, and the parents did not have the authority to make that decision on behalf of the child.

make privacy-related decisions will be determined by the extent of the delegation of the parental responsibility.[187]

68.118 The ALRC notes that the common law provides a limitation on the authority of the parent by requiring that the acts of the parent must advance or protect the welfare of the child.[188] Courts have an inherent *parens patriae* jurisdiction to supervise the care and control of minors by parents and guardians.[189] This limitation on parental authority and court supervision would extend to all persons exercising parental responsibility.

Implementing the age of presumption

68.119 While the ALRC considers that agencies and organisations should give active consideration to establishing a process for individual assessment of the capacity of individuals under the age of 18, it recognises that this is not always reasonable or practicable. Where an agency or organisation seeks to rely on the presumed age of capacity, there should be some obligation on the agency or organisation to determine or verify the age of the individual.

68.120 As discussed in DP 72, the ALRC does not consider that agencies and organisations should be subject to an absolute requirement to establish that an individual is aged 15 or over before relying on the decision of that individual.[190] This would involve a significant compliance burden. Stakeholders supported a limitation on the liability of agencies and organisations in this context.

68.121 The *Privacy Act* should include a provision which balances the obligations of agencies and organisations to verify the age of an individual before relying on the age of presumption of capacity with practical realities. The provision should be couched as a positive obligation on agencies and organisations to take such steps, if any, as are reasonable in the circumstances to verify that the individual is aged 15 or over. This wording incorporates the concept of making a risk assessment—balancing the need to protect the privacy of children and young people, the costs of compliance, and the impact on all clients and customers of the agency or organisation—before deciding what age verification system should be implemented for any specific purpose. The term 'such steps, if any, as are reasonable in the circumstances' has been adopted in a number of the model UPPs.[191]

---

187 For example, it would not be expected that a soccer coach temporarily in charge of the child or young person has the authority to provide consent for the disclosure of a child or young person's personal information to an organisation for commercial purposes. It may be appropriate, however, for a teacher to consent to disclosure of a student's information in order to participate in an online educational activity approved by the school.

188 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218, 316; *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112, 170.

189 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218.

190 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [60.108].

191 See 'Notification' and 'Collection and Access' principles.

68.122 It is not appropriate to prescribe in the *Privacy Act* or subordinate legislation how the age verification mechanisms should be implemented. The market may be expected to continue to develop a range of age verification mechanisms, and there must be sufficient flexibility for agencies and organisations to develop mechanisms that suit their functions and the context in which privacy-related decision making is required.[192] Neither is it feasible for the OPC to spend significant resources monitoring compliance by agencies and organisations. The existence and effectiveness of an age verification mechanism, however, would be an issue for consideration as part of any complaint about a breach of the Act, or as part of an audit of compliance.

Guidance

68.123 The ALRC recommends that the OPC develop and publish guidance on the handling of personal information of individuals under the age of 18. A number of issues have been raised in this chapter where guidance will be required to assist agencies and organisations to interpret and comply with their obligations under the recommended provisions of the *Privacy Act*. These issues include:

- how to involve children, young people, their parents and others with parental responsibility in decision-making processes. This includes providing reasonable assistance to individuals to understand and communicate decisions, and encouraging parental support where this is appropriate;
- when it is reasonable and practicable to undertake individual assessment of the capacity of a child or young person;
- appropriate practices for undertaking individual assessments;
- what constitutes reasonable steps to verify the age of an individual where the agency or organisation seeks to rely on the age of presumption of capacity, including when it may be reasonable to have no age verification mechanism in place; and
- appropriate practices for seeking consent from a person with parental responsibility on behalf of a child or young person lacking capacity, and identification of categories of persons that normally would be considered to have parental responsibility.

192 This regulatory approach has been adopted by the Australian Communications and Media Authority in relation to age verification processes to be developed for the purposes of restricting under-age access to material rated as R18+ or MA15+: Explanatory Statement, Restricted Access Systems Declaration 2007 (Cth), 8–9.

Privacy Policies and training requirements

68.124 One of the themes highlighted by stakeholders was a lack of knowledge and experience on the part of agencies and organisations when dealing with children and young people. The ALRC recommends, therefore, a number of practical solutions to raise the level of awareness of the proposed provisions and improve their practical application.

68.125 In Chapter 24, the ALRC recommends that agencies and organisations develop and publish a Privacy Policy that sets out how the agency or organisation manages personal information and how personal information is collected, held, used and disclosed.[193] Agencies and organisations that handle the personal information of individuals under the age of 18 should address in their Privacy Policies how such information is managed. Issues addressed could include: whether an individual assessment of capacity is carried out and by whom; what age verification mechanisms (if any) are used; and how a person with parental responsibility may act on behalf of a child or young person lacking capacity.

68.126 Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should ensure that their staff are trained adequately to deal with issues concerning the capacity of children and young people. The ALRC notes concerns of stakeholders regarding the compliance burden associated with this recommendation. The ALRC has worded the recommendation to apply only to relevant staff, and has not included a requirement that staff be trained to conduct capacity assessments. It is noted, however, that staff in agencies and organisations that regularly deal with children and young people must become familiar with issues concerning capacity and how that agency or organisation deals with those issues.[194] Where individual assessments are reasonable and practicable, certain staff will need to be trained to undertake such assessments appropriately. Where individual assessments are not routinely undertaken, staff should be made aware of the steps to be taken to determine if an individual is 15 years old or over, and what must occur if an individual is under that age.

Recommendation 68–1 The *Privacy Act* should be amended to provide that where it is reasonable and practicable to make an assessment about the capacity of an individual under the age of 18 to give consent, make a request or exercise a right of access under the Act, an assessment about the individual's capacity should be undertaken. Where an assessment of capacity is not reasonable or practicable, then an individual:

193 See Recs 24–1, 24–2.

194 For a similar discussion on staff awareness regarding issues concerning capacity in adult clients and customers, see Ch 70.

(a) aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and

(b) under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access.

Recommendation 68–2 The *Privacy Act* should be amended to provide that where an individual under the age of 18 is assessed or presumed to not have capacity under the Act, any consent, request or exercise of a right in relation to that individual must be provided or made by a person with parental responsibility for the individual.

Recommendation 68–3 The *Privacy Act* should be amended to provide that, in order to rely on the age-based presumption, an agency or organisation is required to take such steps, if any, as are reasonable in the circumstances to verify that the individual is aged 15 or over.

Recommendation 68–4 The Office of the Privacy Commissioner should develop and publish guidance for applying the new provisions of the *Privacy Act* relating to individuals under the age of 18, including on:

(a) the involvement of children, young people and persons with parental responsibility in decision-making processes;

(b) situations in which it is reasonable and practicable to make an assessment regarding capacity of children and young people;

(c) practices and criteria to be used in determining whether a child or young person is capable of giving consent, making a request or exercising a right on his or her own behalf, including reasonable steps required to verify the age of an individual;

(d) the provision of reasonable assistance to children and young people to understand and communicate decisions; and

(e) the requirements to obtain consent from a person with parental responsibility for the child or young person in appropriate circumstances.

Recommendation 68–5 Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should address in their Privacy Policies how such information is managed and how the agency or organisation will determine the capacity of individuals under the age of 18.

Recommendation 68–6 Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should ensure that relevant staff receive training about issues concerning capacity, including when it is necessary to deal with third parties on behalf of those individuals.

69. Particular Privacy Issues Affecting Children and Young People

Contents

Introduction

69.1 Overall, the ALRC considers that the privacy principles, combined with the recommendations in Chapter 68 relating to decision making by and for individuals under the age of 18, provide adequate protection for the privacy of children and young people. This chapter highlights a number of particular issues and contexts in which privacy issues arise in relation to individuals under the age of 18, and considers whether any additional protections are required within the *Privacy Act*.

69.2 A key area of concern is the interaction between direct marketers and children, particularly in the online environment. The ALRC does not suggest a complete ban on direct marketing to children and young people. It is recommended, however, that the 'Direct Marketing' principle include additional protections for children and young people under the age of 15.

69.3 Another area considered in this chapter is the handling of personal information in schools. While the ALRC does not recommend any legislative change specific to schools, it is recommended that schools clarify certain issues in their Privacy Policies—in particular, the disclosure of student information to parents, and the responsibilities of school counsellors to disclose information to school management and parents.

69.4 Privacy issues in the areas of child care, criminal law, family law and child welfare are also considered. In these areas, the ALRC has highlighted some privacy concerns, but does not consider it appropriate to amend the *Privacy Act* to deal with them. Suggestions are made for further consideration of these concerns by other bodies.

69.5 Another area of concern is the taking of photographs and other images and, in particular, the online publication of photographs and other images. While the issues are not limited to photographs and images of children and young people, many of the examples and particular concerns have related to children and young people. These issues potentially raise problems of a criminal nature as well as concerns regarding invasion of privacy. With a focus on privacy, this chapter canvasses a number of reform options, but does not make any specific recommendations relating to the taking and publishing of photographs and other images. Instead, the chapter links to discussion and recommendations in other chapters that the ALRC considers will provide the most effective remedies, in particular the recommendations for a statutory cause of action for a serious invasion of privacy discussed in Chapter 74.

69.6 Another privacy issue affecting children and young people is the way in which the media handles the personal information of individuals under the age of 18. This issue is discussed in Chapter 42 in the context of the journalism exemption from the *Privacy Act*.

Online consumers and direct marketing issues

69.7 Personal information collected in the online environment is subject to the same laws as any other personal information. This chapter focuses on personal information collected in the online environment, such as through registration pages, survey forms, order forms, and online contests. In Chapter 9, the ALRC discusses technology that can be used to capture personal information in ways that are not obvious to the online consumer, such as by using cookies or web bugs, and security issues in the online environment. In Chapter 67, the ALRC deals more specifically with the situation where a child or young person, or a third party, chooses to disclose personal information on a social networking site.

69.8 The internet is now an integral part of modern marketing techniques. Given their familiarity and high usage of the internet, and their significant consumer power,[1] it is not surprising that this medium is used to target children and young people.

> The World Wide Web has provided children with abundant new opportunities for learning, communicating and playing. But parents and children need to be aware that the Internet has joined television, radio and print as a key component of today's marketing campaigns and many use consumer information to build individual relationships. Children are often more cyber-savvy than their parents. But they also have a trusting and curious nature that may lead them to give out personal information without realising it.[2]

69.9 There is extensive literature that addresses the particular susceptibilities of children as consumers.[3] When combined with a medium that is often used by children and young people with little or no supervision, concerns arise about the privacy of children and young people as consumers using the internet.

Online privacy regulation in Australia

69.10 The *Privacy Act* does not distinguish between the application of privacy principles in the online environment and their application in any other area. There is

---

1 See Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [2.25]–[2.28], [11.1]–[11.2].

2 Australian Direct Marketing Association, *Children and the Internet* (2005) <www.adma.com.au> at 8 April 2008.

3 See, eg, D Kunkel and others, *Report of the APA Task Force on Advertising and Children* (2004) American Psychological Association; R Stanton, 'Into the Mouths of Babes: Marketing to Children' (Paper presented at Cutting Edge: Food and Nutrition for Australian Schools Conference, Brisbane, 18 April 1998); S Beder, *Marketing to Children* (1998) University of Wollongong <www.uow.edu.au/arts/sts/sbeder/children.html> at 10 April 2008; Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [11.60]; Federal Bureau of Consumer Affairs, *Final Report: Advertising Directed at Children* (1995). See also Young Media Australia, *Fact Sheets—Effects of Advertising Directed at Children* <www.youngmedia.org.au/publications/fact_sheets.htm> at 16 April 2008.

some criticism, however, of the operation of the privacy principles in the online environment.

> The fact is that, under existing Australian law, individuals have almost no privacy 'rights' in the online environment and even the few rights they allegedly have are not protected adequately and are difficult, sometimes impossible, to have enforced. The lack of rights arises from a combination of factors, including but not limited to, uncertainty regarding the definition of 'personal information'; no requirement to obtain consent before collecting personal information; use of bundled 'consents' including to disclose information to unspecified 'partners'; the small business exemption; and/or technological developments.[4]

69.11 The more general issue of regulation of the internet is addressed in Chapter 11. The ALRC does not recommend, however, that privacy in the online environment be regulated separately from other environments. The same set of privacy principles is recommended to apply to the handling of personal information regardless of the medium.[5]

69.12 It is possible for industries to develop their own standards or guidelines, consistent with the *Privacy Act*, that address particular online privacy practices, including with respect to the privacy of children and young people. For example, the Internet Industry Association (IIA) has developed a Privacy Code of Practice, which is currently under consideration by the Office of the Privacy Commissioner (OPC).[6] The Code includes a specific provision requiring that a legal guardian provide consent on behalf of an individual under the age of 13 before disclosure of sensitive information collected from or about the child.[7] The Australian Direct Marketing Association (ADMA) publishes tips on helping parents to safeguard a child's privacy online, and plans to introduce guidelines on children's privacy that will be compulsory for its members.[8]

Online privacy regulation in the United States

69.13 While the United States (US) does not have federal legislation for the online privacy of adult consumers, it does have federal online privacy legislation dealing specifically with children. Based on the recommendations of the US Federal Trade Commission (FTC),[9] the *Children's Online Privacy Protection Act 1998* (COPPA) was passed by the US Congress in 1998 with a requirement that the FTC issue and enforce rules concerning children's online privacy.

---

4 Electronic Frontiers Australia Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

5 Rec 18–1.

6 The 2001 draft version of the Code, which was circulated for consultation prior to submission to the OPC in March 2003, can be found at <www.iia.net.au>.

7 Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001), [6.7]. The term 'child' is defined in [5.1].

8 Australian Direct Marketing Association, *Children and the Internet* (2005) <www.adma.com.au> at 8 April 2008.

9 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998).

69.14 The *Children's Online Privacy Protection Act Rule* (COPPA Rule), which came into effect in April 2000, aims to give parents control over what information is collected from their children online. The COPPA Rule applies to operators of commercial websites and online services directed to individuals under the age of 13 that collect personal information from children, and to operators of general websites with 'actual knowledge' that they are collecting information from individuals under the age of 13. Websites hosted in a foreign jurisdiction must comply with COPPA if they are directed to children in the US, however difficult this is to enforce in practice. Under the Rule, operators are required to:

- post a clear and comprehensive privacy policy on their websites;
- provide notice to parents and, with limited exceptions, obtain verifiable parental consent before collecting personal information;
- give parents the choice to consent to the collection and use of personal information about their child;
- provide parents with access to their child's personal information in order to review or delete it;
- give parents the opportunity to prevent further collection or use of the information; and
- maintain the confidentiality, security and integrity of information they collect from children.

69.15 The FTC has a sliding scale approach to obtaining verifiable parental consent, with the requirements for obtaining consent becoming more rigorous where the intended use of the information involves disclosure to third parties rather than internal use. Where the information is to be used for internal purposes only, verifiable parental consent can be obtained through the use of an email message to the parent, coupled with additional steps to provide assurances that the person providing the consent is, in fact, the parent. More rigorous methods specified in the Rule include: fax- or mail-back forms; credit card transactions; staffed toll-free numbers; digital certificates using public key cryptography; and emails accompanied by a PIN or passwords.

69.16 Website operators who violate the COPPA Rule can be liable for civil penalties of up to US$11,000 per violation. The FTC has undertaken an active enforcement approach to COPPA, including 11 successful enforcement cases between 2000 and

2004,[10] and the publication of a survey of the compliance levels of 144 key US websites.[11] In March 2006, after a public review of the Rule, the FTC announced that the COPPA Rule had succeeded in providing greater protection to children's personal information online, and that the Rule—complete with the sliding scale—was to be retained without amendment.[12]

69.17 There have been criticisms, however, of the COPPA Rule and how it has operated in practice. These include that:

- non-profit organisations are not covered by COPPA;[13]
- operators of general websites without 'actual knowledge' of the age of the child do not have to comply with COPPA, and so can circumvent the Rule merely by not asking the age of the person submitting personal information;[14]
- it is easy for children to circumvent the law by lying about their age, or opening email accounts in their parents' names and giving consent on their own behalf;[15]
- the substantial burden of complying with COPPA has forced many websites simply to eliminate children's programming;[16] and
- even those websites complying with the COPPA Rule do not necessarily comply with the spirit of the law, and most existing privacy policies are too complex for children or parents to understand.[17]

---

10 All of these cases were settled. For details see the FTC website: US Federal Trade Commission, *Privacy Initiatives* <www.ftc.gov/privacy/privacyinitiatives/children_enf.html> at 8 April 2008. See also details of more recent settlements against social networking sites Xanga.com and imbee.com: D Caterinicchia, 'Xanga Settles with FTC for $1 Million', *Houston Chronicle* (online), 7 September 2006, <www.chron.com>; United States Federal Trade Commission, 'Imbee.com Settles FTC Charges Social Networking Site for Kids Violated the Children's Online Privacy Protection Act; Settlement Includes $130,000 Civil Penalty' (Press Release, 30 January 2008).

11 Conducted one year after commencement of the COPPA Rule, the FTC found that 90% of the surveyed websites provided a privacy policy that complied with the basics of the Rule. More than half of the websites, however, did not implement fully other aspects of the Rule—for instance, the prohibition on operators making a child's participation in an online activity conditional on the child providing more information than is reasonably necessary to participate in that activity, and the provision requiring parents to be informed of rights to review, delete and refuse further collection and use of their child's personal information: United States Government Federal Trade Commission, *Protecting Children's Privacy Under COPPA: A Survey on Compliance* (2002), i–ii.

12 United States Government Federal Trade Commission, 'FTC Retains Children's Online Privacy Protection (COPPA) Rule Without Changes' (Press Release, 8 March 2006).

13 K Howard and Y Lim, 'Protection of Children in the Virtual World' (2005) 2 *Privacy Law Bulletin* 17, 19.

14 Ibid, 19.

15 M Hersh, 'Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet' (2001) 28 *Fordham Urban Law Journal* 1831, 1870.

16 K Walker, 'The Costs of Privacy' (2001) 25 *Harvard Journal of Law & Public Policy* 87, 125.

17 J Turow, *Privacy Policies on Children's Websites: Do They Play By the Rules?* (2001) Annenburg Public Policy Center of the University of Pennsylvania, 12.

Direct marketing to children and young people

69.18 The Obesity Prevention Policy Coalition (OPPC) and Young Media Australia (YMA) made a joint submission to this Inquiry that focused on the problems of direct marketing aimed at children and young people.[18] Although the concerns about direct marketing arise regardless of the media involved, the increasing use of technology to engage with children and young people was seen as a particular concern.

> In our view, protecting children from interference with their privacy through direct marketing is becoming increasingly important in light of children's increasing use of the internet, email and SMS, and advertisers' widespread use of these technologies to market products directly to children … We are particularly concerned about direct marketing using these technologies because, unlike television, these technologies enable marketers to interact directly with children. Direct marketing using these technologies intrudes directly into children's personal space, and provides marketers with unsupervised access to children.[19]

69.19 The OPPC and YMA cited research indicating that children are more susceptible to commercial influence, and that they are unfairly manipulated by direct marketing.[20] Many children and young people do not have the capacity to make appropriate decisions regarding the disclosure of personal information in a direct marketing context. Further, the OPPC and YMA submitted that direct marketers are unlikely to have the kind of contact with children or young people required to make any individual assessment about capacity. They also noted that direct marketers have a vested interest in assuming that consent is informed and freely given.

69.20 The OPPC and YMA suggested that direct marketers should be prohibited from collecting or using information without the express, verified consent of the child's parent if they know, or would be reasonably likely to know, that it is about an individual under the age of 14. It was proposed that the express, verified consent should be able to be provided through a signed form sent by mail or fax, provision of a credit card number or electronic signature, or calling a toll-free number staffed by trained personnel. It also was suggested that there be a prohibition on making consent to use personal information for direct marketing purposes a condition of entry to a competition, promotion or other activity if the entrant is under the age of 14. The OPPC and YMA provided a number of examples where this condition of entry has been used in competitions or clubs aimed at children in Australia.

---

18 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144*, 25 January 2007.

19 Ibid.

20 See, in particular, D Kunkel and others, *Report of the APA Task Force on Advertising and Children* (2004) American Psychological Association.

Options for reform

69.21 Given the concerns raised about collection of personal information from children and young people for direct marketing purposes, particularly in the online environment, there is a need to consider whether the *Privacy Act* or related legislation should contain additional protections for children and young people that modify the general application of the privacy principles.

69.22 One option is to adopt a model based on COPPA. Many aspects of COPPA apply general privacy measures that are necessary due to the absence of general information privacy legislation in the US. These requirements—including posting privacy policies on websites; rights of access and correction; and obligations to maintain the confidentiality, security and integrity of collected personal information—apply under the *Privacy Act* to all personal information, not only to personal information about children.

69.23 The major additional protections provided by COPPA, which appeal to some in the Australian community, are the requirements to obtain verifiable parental consent before collecting any personal information from an individual under the age of 13, and giving parents the opportunity to prevent further collection or use of the information. This was the basis of the proposed amendment for the 'special protection for children' put forward by the Australian Labor Party during debate on the Privacy Amendment (Private Sector) Bill 2000 (Cth), although the proposal was not limited to online activity as it is in COPPA.[21]

69.24 The suggestion for additional protections stems from concerns that children and young people are unable to make an informed choice before providing personal information to an agency or organisation. For example, a child or young person is more likely than an adult to complete an online form and provide personal information in order to continue to play a game or enter a competition without giving appropriate consideration to the intended use of the personal information. Even where a child or young person stops to consider the consequences, he or she is less likely than an adult to find and understand the privacy policy of the agency or organisation.[22] Combined with the knowledge that children and young people interact regularly with agencies and organisations in the online environment, sometimes without adult supervision, this is seen as a serious concern by some stakeholders.

69.25 Under the model Unified Privacy Principles (UPPs), it is not necessary to obtain an individual's consent to collect his or her personal information, except in relation to sensitive information where no other exception allows for collection without consent. While consent is not required for collection of non-sensitive personal information, an

---

21 Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2006, 20302 (N Bolkus).

22 Dubit Research, *Data Protection—Topline Report [commissioned by United Kingdom Information Commissioner's Office]* (2007). See also research discussed in Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144*, 25 January 2007.

individual often can choose to take steps to prevent an agency or organisation from collecting that personal information. This was one factor considered by the ALRC when making a recommendation that agencies and organisations should be required to collect personal information directly from an individual wherever reasonable and practicable.[23] The ALRC also makes a number of recommendations aimed at improving the extent and clarity of information made available to individuals about how their personal information will be handled.[24] These recommendations, however, will not be of assistance to a child who is incapable of understanding and synthesising the information in order to make informed choices.

69.26 On the other hand, there are practical reasons why the privacy principles do not require consent to every collection of personal information. There needs to be a balance between privacy protection and the practical operation of services and businesses. Protections where required are included in the UPPs while still allowing for the appropriate flow of information. This may require agencies and organisations to seek consent from individuals where there are particular risks, such as before the collection of sensitive information, and before a use or disclosure that is not consistent with the primary purpose of collection, or otherwise covered by the carefully crafted exceptions to the 'Use and Disclosure' principle. General protections relating to data quality and security apply to all personal information regardless of the way in which it was collected.

Submissions and consultations

69.27 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC considered that the consent mechanisms built into the proposed 'Direct Marketing' principle provided sufficient protection to children and young people. Particularly when combined with the proposals regarding decision making on behalf of individuals under the age of 15, it was considered that no additional protections were necessary.

69.28 As indicated in Chapter 68, ADMA did not support the ALRC's proposals for determining the decision-making capacity of individuals under the age of 18. ADMA was concerned about the impact they would have in the direct marketing context.[25] The Law Council of Australia had a similar reaction:

> There are many organisations that regularly collect and use the information of young people for marketing purposes (for example, birthday clubs, teen magazines, competitions etc), which are perfectly acceptable.
>
> Imposing an age limit in relation to capacity to make privacy related decisions, including consenting to collection of information, would be impracticable and

---

23 See Rec 21–1. This requirement exists in NPP 1.4 in relation to organisations, and the ALRC recommends extending the requirement to apply to agencies.

24 See Ch 23.

25 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

> burdensome for businesses, especially in the online environment, and may deprive young people of opportunities they may otherwise be offered.
>
> Offers are regularly made to young people which involve collection of their personal information. If it is considered that personal information should not be collected in specific circumstances, this should be a matter for the legislature to regulate. The difficulty with the proposed restriction is that it would place a burden on the organisation collecting the information which would be difficult to discharge. This may result in a detriment to young people, as organisations may choose to discontinue these activities.[26]

69.29 The Obesity Policy Coalition, which raised significant concerns about direct marketing to children in an earlier submission to the Inquiry, gave general support for the proposed 'Direct Marketing' principle—in particular the requirement to obtain parental consent on behalf of a child or young person lacking decision-making capacity.[27] The Coalition was worried, however, that the proposed principle provides too broad an exception that may allow direct marketing to children without parental consent. Of major concern was the exception in the 'Direct Marketing' principle that allows for direct marketing using non-sensitive personal information without consent where it is impracticable for the organisation to seek consent.[28]

69.30 In DP 72, the ALRC suggested that guidance should deal with this issue, requiring the establishment of appropriate age verification and parental consent mechanisms where an organisation 'knowingly' handles personal information relating to individuals under the age of 15. The Obesity Policy Coalition submitted that the principle and guidance imposed insufficient obligations on organisations, too easily allowing an interpretation to avoid the consent requirement where 'it is difficult to identify, locate or communicate' with the person with parental responsibility.[29]

69.31 The Obesity Policy Coalition also was concerned about the effective operation of the opt out provisions of the 'Direct Marketing' principle. While giving general support for the inclusion of opt out provisions, and the ability for a person with parental responsibility to activate the opt out on behalf of an incapable child or young person, the Coalition suggested that ongoing communications directly between the organisation and the child or young person would hinder the ability for the person with parental responsibility to exercise the option at an appropriate time. The Coalition suggested that those acting on behalf of the child or young person should be given the option to opt out directly each time information is communicated to that child or young person.[30]

---

26 Law Council of Australia, *Submission PR 527*, 21 December 2007.

27 Obesity Policy Coalition, *Submission PR 506*, 20 December 2007. Note that the Obesity Policy Coalition is the new name for the Obesity Prevention Policy Coalition that made an earlier submission to this Inquiry.

28 See UPP 6.1(a), as proposed in DP 72.

29 Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.

30 Ibid.

69.32 Liberty Victoria also did not support the 'one-size-fits-all' approach of the proposed 'Direct Marketing' principle, or the guidance for dealing with vulnerable individuals including children. It suggested that there was a need for a positive obligation on direct marketers not to 'manipulate' children.[31]

ALRC's view

69.33 When combined with the ALRC's recommended provisions regarding decision making by and on behalf of individuals under the age of 18, the balance provided in the privacy principles between privacy protection and the free flow of information is appropriate and gives adequate protection to the personal information of a child or young person.

69.34 The ALRC notes particular concerns, however, about direct marketing. Questions may be raised about whether direct marketing to children and young people, of itself, is undesirable. The OPPC and YMA presented evidence highlighting that, for developmental reasons, children and young people are less able to resist commercial influence and that the risks to children are heightened when combined with technology that enables organisations to contact children directly.[32] It is not appropriate to prohibit direct marketing to children and young people through information privacy law. Such a decision must involve policy considerations that extend beyond the scope of this Inquiry. The recommendations in this Report will ensure, however, that personal information about children and young people is handled appropriately by direct marketers.

69.35 The ALRC has reconfigured the 'Direct Marketing' principle, in light of concerns raised by stakeholders in response to DP 72.[33] The recommended principle imposes different obligations on organisations based on a distinction between unsolicited direct marketing and direct marketing to existing customers. Direct marketing to existing customers is a simpler process that does not require the individual's consent (or the application of the exception to seek consent).

69.36 In redrafting the principle, the ALRC considered the level of protection that exists for children and young people. Part of the ALRC's reasoning in DP 72 for *not* proposing additional protections for children and young people in relation to direct marketing was that the proposed principle operated to require parental consent before using personal information about child or young person lacking decision-making capacity for the purposes of direct marketing. The ALRC acknowledged that the exception to consent—ie, where it is non-sensitive information and it is impracticable to obtain consent—would apply, but proposed guidance from the OPC to indicate how

---

31 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.
32 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144*, 25 January 2007.
33 See Ch 26.

the exception would operate to limit the circumstances in which an organisation could claim it is impracticable to obtain parental consent.[34]

69.37 Parental consent generally should be a prerequisite to the use of personal information for direct marketing purposes of a child or young person lacking decision-making capacity. While overall the ALRC considers that the obligations imposed on direct marketers in relation to existing customers can be reduced, due to the ongoing relationship between the organisation and customer,[35] this policy is inappropriate when dealing with children and young people lacking decision-making capacity. Evidence has shown that children and young people have greater difficulties in distinguishing between commercial and non-commercial content. While children over the age of eight may have a rudimentary understanding that advertising is intended to sell products, many are unable to interpret advertising messages critically and understand the persuasive intent.[36]

69.38 For these reasons, the ALRC has built into the 'Direct Marketing' principle an additional protection for individuals under the age of 15, requiring that these children and young people never be treated as 'existing customers' for these purposes.[37] This brings into play higher obligations on the organisation seeking to use personal information about the individual for the purposes of direct marketing in relation to each use of the information—that is, the consent of the individual must be obtained for the use, unless the information is non-sensitive personal information, and it is impracticable to seek consent. When combined with the ALRC's recommendations relating to decision making for children and young people lacking decision-making capacity, this will require that a person with parental responsibility provide the consent on behalf of the child or young person.[38]

69.39 The ALRC notes that incorporating an age cut off of 15 years, which is the age of presumption of capacity recommended in Chapter 68, varies from the ALRC's recommendations that the capacity of an individual under the age of 18 should be assessed whenever reasonable and practicable. It is recognised that in almost all circumstances involving direct marketing it would be unreasonable or impracticable for the organisation to undertake an individual assessment of the capacity of the individual. By incorporating the age of presumption of capacity in relation to this particular use of personal information, the wording of the principle is kept as simple as possible. This is consistent with the ALRC's general approach to the drafting of the privacy principles, while still meeting the ALRC's overall policy objectives in relation to regulating decision making by and on behalf of individuals under the age of 18 years.

---

34 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [60.136].

35 See discussion in Ch 26.

36 D Kunkel and others, *Report of the APA Task Force on Advertising and Children* (2004) American Psychological Association. See also discussion of the psychological literature in relation to decision-making capacity of children and young people in Ch 68.

37 The 'Direct Marketing' principle is dealt with in detail in Ch 26.

38 See Recs 68–1, 68–2.

69.40 Some stakeholders had concerns about the operation of the 'not practicable' exception to obtaining consent in the 'Direct Marketing' principle and the detrimental effect this could have on organisations implementing appropriate age verification and parental consent mechanisms. The ALRC notes these concerns and considers that it will be necessary to ensure that guidance in relation to the 'Direct Marketing' principle, as well as guidance in relation to the handling of personal information of individuals under the age of 18 years, deals sufficiently with these concerns to ensure that the principle and provisions are implemented appropriately.[39]

Schools

Schools and the *Privacy Act*

69.41 School is the most significant institution in the lives of the majority of children and young people. Schools collect and hold a vast array of personal information regarding children and young people, including names, addresses, family information, subjects studied, grades and behavioural information. Schools often will hold health information about children and young people, either collected directly from the child or young person (or their parents or guardians), or collected as part of a service offered within the school, such as visits to a school dentist, nurse or counsellor. Photos and videos of children and young people taken by the school also fall within the definition of personal information.

69.42 With the exception of the ACT, government schools are not covered by the *Privacy Act* but are subject to any state or territory privacy legislation or scheme covering the public sector. Some states and territories have a privacy policy or privacy code that applies to all of their schools.[40] Further, many schools have developed policies or practices dealing specifically with the publication on their websites of photographs or videos depicting children and young people.[41]

69.43 Private schools are covered by the *Privacy Act* unless they fall within the small business exemption.[42] Even smaller private schools are likely to be partly covered by the *Privacy Act*. Information relating to the provision of a health service, which

---

39 See recommendations in relation to guidance in these areas: Recs 26–7, 68–4.

40 See, eg, South Australian Government Department of Education and Children's Services, *SA Government Schools and Children's Services: Information Privacy Statement* which sets out that the disclosure of personal information is regulated by the South Australian Information Privacy Principles and that access to information about a person may be requested by that person or a parent or guardian of that person.

41 See, eg, Curriculum Materials Information Services, *Protecting Student Privacy* Department of Education and Training Western Australia <www.det.wa.edu.au/education/cmis> at 10 April 2008, which suggests that parental consent should be sought when photographs or digital images of students are to be used outside the classroom environment, eg, in the local community newspaper, or on a website or CD-ROM promoting the school. Some schools seek the student's consent as well, although this is not a uniform policy.

42 Note that the ALRC recommends the removal of the small business exemption from the *Privacy Act*: see Rec 39–1.

includes physical education classes or fitness instruction, as well as services provided by nurses and other health professionals, is regarded as 'health information' and is regulated by the Act.[43] The OPC takes the view that, in most instances, private schools and colleges are covered by the Act and should comply with the National Privacy Principles (NPPs).[44]

69.44 One of the key issues relating to access to the records of a child or young person is whether the school can disclose a record to a parent or guardian. In the private school context, it is generally the parents or guardians who enter into a contract with the school to provide a service. Schools subject to the NPPs, however, must disclose personal information regarding the child or young person only in accordance with the NPPs.

69.45 Advice from the OPC suggests that most personal information collected by a private school may be disclosed to parents under NPP 2.1(a), as in most cases students reasonably would expect disclosure of the information to parents. The OPC indicates that generally students would expect the disclosure of school reports, and also material not related to education, such as health information or counselling records.[45] For older students, however, these expectations may differ in relation to some records containing sensitive information. The OPC suggests that it is good practice, particularly in respect of older students, for schools to have a policy on the disclosure of records to parents.[46] This policy also should be made available to parents and students. A number of policies relevant to government schools suggest that parents should have access to their child's records, at least until the child turns 18.[47]

Issues regarding handling of personal information by schools

69.46 A number of bodies that act on behalf of children and young people made submissions to the Inquiry highlighting concerns about privacy in schools. The concerns included:

---

43 Office of the Privacy Commissioner, *FAQs: Are Private Schools and Colleges Covered by the New Private Sector Provisions* <www.privacy.gov.au/faqs/cf/q3.html> at 10 April 2008.

44 Ibid.

45 Office of the Privacy Commissioner, *FAQs: Can Private Schools Disclose Non-education Related Personal Information about Students to Their Parents?* <www.privacy.gov.au/faqs/cf/q6.html> at 10 April 2008; Office of the Privacy Commissioner, *FAQs: Can Parents Whose Children Attend a Private School/College Still Get Access to Their Children's School Reports?* <www.privacy.gov.au/faqs/ypr/q15.html> at 10 April 2008. The Office of the Victorian Privacy Commissioner has given similar advice in relation to school reports in Victoria: Office of the Victorian Privacy Commissioner, *Privacy and School Reports: Fact Sheet 02.02* (2002).

46 Office of the Privacy Commissioner, *FAQs: Can Private Schools Disclose Non-education Related Personal Information about Students to Their Parents?* <www.privacy.gov.au/faqs/cf/q6.html> at 10 April 2008.

47 See South Australian Government Department of Education and Children's Services, *SA Government Schools and Children's Services: Information Privacy Statement*; ACT Department of Education & Training and ACT Children's Youth & Family Services Bureau, *School Policy: Access to Student Records: Policy and Implementation Guidelines* (2003).

- inconsistencies in privacy policies and practices at different schools;[48]

- increasing amounts of personal information being collected by schools for risk management purposes. It has been suggested that while the collection is being done with consent, there are increased dangers of inappropriate disclosure;[49]

- examples of private schools contracting away a student's right to privacy in a standard form agreement with fee paying parents for the provision of education to the student;[50]

- intrusive practices that breach privacy, sometimes supported by school policies;[51]

- the interpretation of NPP 2 by schools to justify disclosure without consent of personal information about students to parents, on the basis that it is a disclosure reasonably expected by the student. It was submitted that the views, age and maturity of each student should be taken into consideration, and the student should be given the opportunity to object to disclosure in particular circumstances;[52]

- the need for funding for schools to develop and implement clear privacy policies, including informing parents of the privacy rights of students, and the development of a school privacy audit tool to measure how effectively students' privacy is being respected and protected;[53] and

- the need for stronger sanctions for schools failing to adhere to privacy laws.[54]

69.47 The Australian Privacy Foundation raised concerns about the increasing use of technology in schools involving the collection and storage of personal information—such as fingerprinting for school library services, swipe cards for monitoring attendance, and the use of closed-circuit television (CCTV) for security purposes.[55] The Australian Privacy Foundation noted that such technology is often introduced for

---

48 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.

49 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

50 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

51 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.

52 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

53 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.

54 Youthlaw, *Submission PR 152,* 30 January 2007.

55 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also H Edwards, 'The Digital Finger is Pointing at Truants', *Sun Herald* (online), 22 October 2006, <www.fairfax.com.au>.

administrative convenience with little regard for privacy concerns. It argued that further consultation on such developments should be undertaken before such technology is introduced.[56]

69.48 The National Catholic Education Commission (NCEC) and the Independent Schools Council of Australia (ISCA) provided the ALRC with a copy of their *Privacy Compliance Manual*, which was developed in conjunction with the OPC.[57] The NCEC and ISCA indicated that the Manual has been an effective tool in assisting non-government schools to comply with the *Privacy Act*, and that there have been very few expressions of concern to those bodies about infringements of privacy.

69.49 The NCEC and ISCA indicated that schools rely on the consent of a parent (regardless of the age of the student) to collect a student's personal information.[58] On the issue of disclosure of personal information about students to parents, the NCEC and ISCA suggested that schools should be able to use a 'best interests of the student' test to determine whether personal information should be disclosed.[59]

69.50 The NCEC and ISCA raised a number of other circumstances in which the *Privacy Act* and the NPPs makes it difficult for schools to comply with privacy laws. For example, it was suggested that the existing exceptions to allow refusal of access to an individual's record were too limited to cover the full range of circumstances in which access should be able to be refused.[60] These concerns were considered by the ALRC in developing the 'Use and Disclosure' principle.[61]

69.51 The NCEC and ISCA also noted provisions in New South Wales and Queensland legislation that authorise the transfer between schools of personal information about a student, without the consent of the student or the student's parent or guardian, before enrolment of the student in a new school.[62] The purpose of the provisions is to allow the new school properly to assess behavioural issues and

---

56 See recent concerns in New South Wales schools over implementation of attendance systems using fingerprint scanning: A Patty, 'School Forced to Halt Fingerprint Roll Call', *Sydney Morning Herald* (online), 4 April 2008, <www.smh.com.au>.

57 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85*, 12 January 2007; National Catholic Education Commission and National Council of Independent Schools' Associations, *Privacy Compliance Manual* (revised 2004 ed, 2001). Between them, the NCEC and ISCA represent around 2,800 schools in Australia with over 1,000,000 students enrolled in those schools.

58 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85*, 12 January 2007.

59 Ibid.

60 Ibid.

61 See Ch 25.

62 *Education Act 1990* (NSW) pt 5A inserted by the *Education Legislation Amendment Act 2006* (NSW)—the provisions have not yet been proclaimed and are not in operation at present; *Education (General Provisions) Act 2006* (Qld) ss 383–389. The Queensland provisions require that copies of the transferred information be provided to the parent of a student or, in appropriate cases, just to the student, but no consent is required prior to transferring the information: *Education (General Provisions) Act 2006* (Qld) s 387.

consider the health and safety of the transferring student and other students in the school. In the past, this kind of information was not always disclosed to the new school due to privacy concerns. The NCEC and ISCA suggested that such a provision should be included in the *Privacy Act*, therefore ensuring the uniform operation across all Australian states and territories. In particular, the provision should cover the interstate transfer of students.[63]

69.52 The ALRC notes that a national protocol has been developed through the Ministerial Council on Education, Employment, Training and Youth Affairs (MCEETYA) to provide for transfer of personal information when students transfer interstate. The protocol covers both government and non-government schools.[64] The protocol provides for transfer of personal information from a government school only with the consent of the parent or guardian and, where the student is aged 16 or over, the consent of the student. Consistent with information privacy laws in most Australian jurisdictions, the protocol suggests that transfer may be possible without consent if required to prevent a serious risk to the student or to public health and safety. The protocol establishes that consent is not required if a non-government school has a data collection notice that complies with the NCEC and ISCA *Privacy Compliance Manual* advising parents, guardians and students that personal and sensitive information may be disclosed to other schools for administrative and educational purposes.[65]

69.53 School counselling is another area where privacy concerns arise. Most secondary schools provide a school counsellor on a full-time or part-time basis, and most primary schools have access to a school counsellor. While school counsellors are an important resource for young people, research suggests that concerns regarding confidentiality are a key reason why young people do not seek the assistance of a counsellor.[66] Policies regarding the confidentiality of school counselling services vary. Counsellors in any environment are subject to restrictions on the confidentiality of their communications. Such restrictions include mandatory reporting obligations under child protection and communicable diseases laws. As employees of a school or education

---

63 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85*, 12 January 2007.

64 The protocol was developed and agreed on by the Australian Government, state and territory education authorities, the independent and Catholic education sectors through MCEETYA. The requirement to use the Interstate Student Data Transfer Note (ISDTN) is set out in the *Schools Assistance (Learning Together—Achieving Through Choice and Opportunity) Act 2004* (Cth) s 31(m). Details of the ISDTN are available at Ministerial Council on Education, Employment, Training and Youth Affairs, *Interstate Student Data Transfer Note* <www.mceetya.edu.au/mceetya/default.asp?id=12095> at 8 April 2008.

65 National Catholic Education Commission and National Council of Independent Schools' Associations, *Privacy Compliance Manual* (revised 2004 ed, 2001), [7.10.1]. As indicated in the *Privacy Compliance Manual*, the standard form data collection notice is intended to ensure that the individual is reasonably aware of the matters specified in NPP 1.3 and to obtain consent for use and disclosure of personal information that may not be regarded as being for primary or secondary related (or directly related) purposes.

66 W Reid, *School Counselling: A Client Centred Perspective* (1996) Kids Help Line, 10.

department, however, many counsellors have to balance the requirement to maintain confidentiality with the demands of principals and teachers who feel they have the right to know what is affecting a particular student.[67]

69.54 Young people involved in the ALRC's youth workshops were adamant that a visit to a school counsellor should be confidential.[68] Many indicated, however, that their impression or experience of school counselling was that confidentiality was limited, either because of the physical limitations of seeking advice from counsellors situated within the school, or because of what was perceived as 'a breach of confidence' occasioned by the disclosure of information to someone else.[69]

69.55 The NCEC and ISCA consider that counsellors employed by schools and related bodies (such as a Catholic welfare agency retained by the school to provide counselling services) have a duty to inform the school principal if the counsellor becomes aware of information that may affect the health or wellbeing of the pupil, and the information is relevant to the school performing its contractual duties to provide schooling. The NCEC and ISCA also believed that the records of school counsellors are the same as any other school record, and that the counsellor could be directed to disclose to the school principal the contents of any record of a discussion.[70] The NCEC and ISCA indicated that some counsellors have suggested that this situation should be changed by legislation to strengthen confidentiality. The NCEC and ISCA noted that they are opposed to any such change.[71]

Discussion Paper proposal

69.56 In DP 72, the ALRC noted that many of the concerns raised about the handling of personal information in schools appear to stem from a combination of poor practices that are inconsistent with privacy principles, and school policies that provide sometimes questionable interpretations of the privacy principles.[72] The ALRC considered that the privacy principles are capable of operating effectively in the school environment and that no specific additional rules were required. The ALRC suggested that there is, however, a need to clarify aspects of the operation of the privacy principles and to ensure appropriate implementation.

69.57 In DP 72, the ALRC proposed that schools clarify in their Privacy Policies how the personal information of students will be handled, and specified two particular areas of concern: when information will be disclosed to, or withheld from, persons with

---

67 Ibid, 8.

68 See also S Akgul, *Submission PR 380*, 6 December 2007.

69 This issue was also raised at Children and Young People Issues Roundtable, *Consultation PC 121*, Sydney, 7 March 2007.

70 This is set out in National Catholic Education Commission and National Council of Independent Schools' Associations, *Privacy Compliance Manual* (revised 2004 ed, 2001), 75.

71 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85*, 12 January 2007.

72 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [60.155].

parental responsibility; and the disclosure of personal information by school counsellors to school management, persons with parental responsibility, and others.[73]

Submissions and consultations

69.58 The ALRC's proposal to clarify certain matters in the Privacy Policies of schools received general support from stakeholders.[74]

69.59 The NCEC and ISCA supported the requirement to set out privacy issues in school policies, and indicated that this is already done.[75] They were concerned, however, that the ALRC's proposals in relation to determining the decision-making capacity of students generally were too restrictive and did not provide schools with sufficient flexibility to make appropriate decisions in appropriate cases. The submission from the NCEC and ISCA set out a number of situations where conflicts may arise between the wishes and interests of students and parents, and the school has to make difficult decisions about which approach to take.

> The School has to consider the rights and expectations of the parent or parents, who are paying the bills and have legitimate interests as parents, the rights and expectations of the student, and the overriding interest of what is best for the student, bearing in mind the School's legal obligation to discharge its duty of care.[76]

69.60 A number of stakeholders gave explicit support to ensuring that schools are subject to the *Privacy Act* and compliance with the privacy principles is improved.[77] For example, the National Children's and Youth Law Centre (NCYLC) submitted that:

> the NCYLC supports the applications of the UPPs to schools. The experience of the teacher-student relationship and the extensive interaction between school and student calls for a high standard of respect for the rights of the child. A school should always

---

73 Ibid, Proposal 60–7.

74 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Australian Government Department of Human Services, *Submission PR 541,* 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495,* 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007; National Children's and Youth Law Centre, *Submission PR 491,* 19 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462,* 12 December 2007; Youthlaw, *Submission PR 390,* 6 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388,* 6 December 2007.

75 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462,* 12 December 2007.

76 Ibid. The situations listed included a pregnant teenager asking the school not to tell her parents about her medical condition, a student reporting fighting at home which is having a significant effect on the student, and a student asking for assistance in arranging a meeting with one parent where the other parent has opposed this.

77 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; National Children's and Youth Law Centre, *Submission PR 491,* 19 December 2007; Youthlaw, *Submission PR 390,* 6 December 2007.

> be in a position to take the views of each child into account and respect the child's right to privacy—no matter what age.[78]

69.61 The need for training of teachers and administrative staff was raised by a number of stakeholders as an important element in improving the understanding of privacy practice and ensuring compliance with privacy legislation.[79] The Law Society of New South Wales also suggested that the OPC should be involved in setting criteria for school policies.[80]

69.62 The ALRC's proposal encompassed all schools, not only schools covered by the *Privacy Act*. The OPC extended its support for the proposal only in relation to schools currently covered by the *Privacy Act*, namely private schools.[81] Privacy NSW indicated that the proposal should apply to all Australian schools, and that the issue should be placed on the agenda of the Council of Australian Governments.[82]

ALRC's view

Privacy policies in schools

69.63 Most schools, education departments and independent bodies representing schools, have privacy policies or more detailed privacy manuals in place. These are essential to provide guidance, and some level of certainty regarding the requirements for the handling of personal information, to individual schools, teachers, students, parents and guardians. The development of a Privacy Policy should be a requirement for every school subject to the *Privacy Act*. The ALRC supports the development of privacy manuals to provide additional guidance. The ALRC is concerned, however, that some of the content of existing policies and manuals is not wholly consistent with the privacy principles and the *Privacy Act*.

69.64 In Chapter 68, the ALRC has made recommendations to recognise the decision-making capacity of children and young people, and allow them to make independent decisions where that capacity is demonstrated. These recommendations are consistent with international obligations and the developing law that recognises the evolving decision-making capacities of children and young people, balanced with parental responsibilities. Privacy policies and manuals in schools should reflect the general approach set out in the ALRC's recommendations that an individual assessment of a child or young person is the most appropriate way to determine his or her decision-making capacity. Some situations in the school environment are suitable for individual assessment, such as in a counselling situation.

---

78 National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.

79 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.

80 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

81 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

82 Privacy NSW, *Submission PR 468*, 14 December 2007.

69.65 There will be situations, however, where it is not reasonable or practicable to undertake individual assessments. In these situations it will be necessary for schools to apply an across-the-board policy—for example, by issuing a consent form. As discussed in Chapter 68, in the absence of an individual assessment, 15 years should be the age at which it is assumed that a young person has the capacity to make decisions under the *Privacy Act*. This recommended age, based on research on child development and adolescent decision-making, was considered the appropriate point at which the vast majority of individuals have the relevant decision-making capacity. Requirements for obtaining consent from students aged 15 or over can be built into consent forms as easily as parental consent requirements.

69.66 This is not to say that every student aged 15 or over should be able to withhold all personal information from his or her parents or guardians. Existing privacy policies and privacy manuals note appropriately that much of the personal information held by schools can be disclosed to parents or guardians as this is the expectation of all parties—either as part of the primary purpose of collection, or a related secondary purpose. School reports are a prime example, and guidance from the OPC supports this interpretation of the privacy principles.[83] School privacy policies should describe clearly the kinds of personal information that are collected, the purpose of collection, and situations where the information will be disclosed routinely to parents and guardians.

69.67 This does not mean, however, that the requirements of the *Privacy Act* can be overridden by a Privacy Policy. The ALRC has particular concerns about suggestions that some schools assume that contracts between parents and a school displace the privacy rights of the student. Any Privacy Policy must be consistent with the law—and in particular privacy principles and the *Privacy Act*. It is possible that contractual arrangements between parents and a school may contextualise the purpose for which certain information is collected by the school. Use and disclosure practices, however, must be undertaken consistently with the operation of the 'Use and Disclosure' principle. Privacy Policies can assist to clarify the purpose of collection and, therefore, the intended use and disclosure of certain types of personal information.

69.68 Some concerns were raised that schools that do not comply with their requirements under privacy legislation are not dealt with effectively under the existing regime. This is of concern if, as has been suggested to the ALRC, some school Privacy Policies and practices are not consistent with the *Privacy Act*. The ALRC has made a number of recommendations aimed at improving compliance of agencies and organisations subject to the Act.[84]

---

83 Federal legislation requires, as a condition of federal funding, that schools provide to parents of each student school reports twice a year on the progress and achievements of the student: *Schools Assistance (Learning Together—Achieving Through Choice and Opportunity) Act 2004* (Cth) s 32.

84 See Ch 50.

School counselling

69.69 The obligations on counsellors to disclose personal information to school management and parents is a particular area in which conflict and inconsistencies in approach appear. Counsellors and students want as few limitations as possible on the confidentiality of the service, enabling counsellors to develop a level of trust and confidence with students. This must be balanced, of course, with the needs of the school to meet its obligations to provide support for the individual student, and to protect that student and the broader student body.

69.70 In addition to mandatory reporting requirements imposed by child protection legislation, the *Privacy Act* should contain appropriate exceptions that allow disclosure of personal information without consent of the individual—including in circumstances where there is a serious threat to an individual's life, health or safety; or to public health or public safety. The exceptions do not use school-specific language, but they adequately cover situations likely to be encountered in schools.

69.71 School privacy policies should set out clearly the limits of the confidentiality of school counselling services, and indicate circumstances and give examples—consistent with the privacy principles and any additional legislative obligations—in which personal information collected by school counsellors will be disclosed to the school management, persons with parental responsibility, and others. This will include where counsellors are subject to mandatory reporting requirements under child protection legislation, and where disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety, or public health or public safety.

Applying the requirements to state and territory government schools

69.72 The ALRC agrees with stakeholders that the rules and policies regarding handling of personal information in schools should be consistent across all Australian schools. The ALRC, however, has not extended the recommendation to impose obligations on government schools that are not subject to the *Privacy Act*.

69.73 Elsewhere in this Report the ALRC recommends that the states and territories adopt the model UPPs and key definitions in the *Privacy Act*. This should ensure that nationally consistent laws relating to the handling of personal information are in force across Australia.[85] In particular, the same principles will apply across all schools, public and private. A further step is required to develop consistent privacy policies.

69.74 As noted above, MCEETYA has developed a national protocol to provide for the transfer of information when students transfer interstate, encompassing both public and private schools. The ALRC considers MCEETYA the appropriate body to develop a nationally consistent approach to the handling of personal information in schools.

---

85 See discussion in Ch 3.

69.75 Pending the implementation of the ALRC's recommendations aimed at achieving nationally consistent privacy regulation, there are enough similarities in the privacy principles across the country to enable the development of a consistent protocol to apply in the school context. A consistent protocol for the handling of personal information also would facilitate the transfer of personal information between schools across state and territory borders. This will not require all schools to have identical privacy policies, but individual privacy policies based on the national protocol will ensure greater consistency.

Recommendation 69–1 Schools subject to the *Privacy Act* should clarify in their Privacy Policies how the personal information of students will be handled, including when personal information:

(a) will be disclosed to, or withheld from, persons with parental responsibility and other representatives; and

(b) collected by school counsellors will be disclosed to school management, persons with parental responsibility, or others.

Recommendation 69–2 The Ministerial Council on Education, Employment, Training and Youth Affairs should consider the handling of personal information in schools, with a view to developing uniform policies across the states and territories consistent with the *Privacy Act*.

Child care services

69.76 A growing number of Australian children come into contact with formal child care before commencing school.[86] Vacation and before and after school care is also provided by child care services for school aged children. As with schools, child care services collect a large amount of personal information about a child, and his or her family, in order to provide a service.

69.77 A wide range of formal child care services are available, and each has a different structure. They include community-based non-profit services, services administered by local councils, individuals providing care in their own homes, privately owned and managed centres (including some owned by publicly listed companies), and services

86 In 2005, 53% of three year olds were receiving some form of formal child care. Overall, for children aged 0–11, formal care (either alone or in combination) was used by 23% of children, up from 19% in 2002 and continuing the upward trend observed since 1996: Australian Bureau of Statistics, *Child Care, Australia, 2005*, 4402.0 (2006).

provided by employers attached to the workplace of parents. Regulation of the sector is shared between the Australian Government and the states and territories.

69.78 The application of privacy laws to the child care sector is confusing.[87] Larger private or non-profit businesses running child care centres are subject to the NPPs, but many smaller centres, most non-profit services and individuals running a service within their own home would fall within the small business exemption to the *Privacy Act*.[88] Some otherwise exempt small businesses, however, may fall within the definition of a health service provider under the *Privacy Act* or state health information legislation. Services operated by a state, territory or local council are subject to any relevant state or territory privacy legislation or scheme.[89]

69.79 National standards have been developed for child care services, and have been utilised to inform child care regulations, funding guidelines and information resources.[90] The degree of implementation has varied between jurisdictions. Each set of standards includes a standard on maintenance of records listing the information (most of which would fall within the definition of personal information) that must be kept confidential, although they differ on when that information may be disclosed.[91] Some child care centres have their own privacy policies in place to govern the collection, use and disclosure of personal information.

---

87 Until 2000, child care service providers that received Commonwealth funding had to enter a contract with the Commonwealth and thus provided services under contract to the Commonwealth, attracting the application of the IPPs. Due to a change in funding arrangements, this is no longer the case.

88 Note that the ALRC recommends the removal of the small business exemption from the *Privacy Act*: see Rec 39–1.

89 For a discussion of the different privacy regimes that may be applicable to a child care service, see K Flanagan, *Privacy in NSW Children's Services* (2002) Community Child Care Co-operative <www.ccccnsw.org.au/facts> at 10 April 2008.

90 See Children's Services Sub-Committee, *Standards for Centre Based Long Day Care* (1993) Australian Government Department of Families, Community Services and Indigenous Affairs; Children's Services Sub-Committee, *National Standards for Family Day Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs; Children's Services Sub-Committee, *National Standards for Outside School Hours Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs. All of the Standards can be found at <www.facsia.gov.au>. These Standards are currently under review: see Community and Disability Services Ministers' Conference, *A Review of the Approach to Setting National Standards and Assuring the Quality of Care in Australian Childcare Services* (2006).

91 The Standards for centre-based long day care indicate that records should be kept up-to-date and in a 'safe and secure area', that they 'remain confidential' and only made available 'to those who have a genuine interest' in obtaining the record: Children's Services Sub-Committee, *Standards for Centre Based Long Day Care* (1993) Australian Government Department of Families, Community Services and Indigenous Affairs, 5.3.1. The Standards for family day care are similar but only allow that records be made available 'to those who have a lawful right to them': Children's Services Sub-Committee, *National Standards for Family Day Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs, 4.3.1. The Standards for outside of school hours care are silent on the issue of disclosure: Children's Services Sub-Committee, *National Standards for Outside School Hours Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs, 5.3.2.

69.80 For the administration of payments under the Child Care Benefit scheme, child care services are required to transfer information about child attendances to the Department of Education, Employment and Workplace Relations.[92] The information requirements have become more rigorous since the introduction of the Child Care Management System, which is designed to make the industry more accountable.[93] Information held by the Department is subject to the *Privacy Act*, and staff are also subject to the confidentiality provisions of the *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth).[94]

Submissions and consultations

69.81 The Department of Families, Community Services and Indigenous Affairs was previously responsible for the Child Care Management System, and submitted to this Inquiry that the specific privacy and secrecy provisions in family assistance law provide adequate privacy protection for personal information transferred to the Government by child care services.[95] The NCYLC indicated that the application of privacy laws is confusing in the area of child care services, given the variety of services, varying regulatory mechanisms and the possible range of applicable privacy laws.[96] The NCYLC supported a national strategy to review privacy policies and standards in child care services.

ALRC's view

69.82 Most of the concerns about the handling of personal information in child care services stem from the broad range of services available, the varying regulatory structures applied to the services, and the resulting confusion about the applicable privacy requirements. The ALRC's recommendations to achieve nationally consistent information privacy laws across federal, state and territory jurisdictions will help substantially in reducing the confusion by ensuring that consistent privacy principles apply regardless of the regulatory structure in place for the particular child care service.[97] In the absence of more specific concerns about the handling of personal information in child care services, the ALRC does not recommend specific reform in this area.

---

92 This information was previously provided to the Australian Government Department of Families, Community Services and Indigenous Affairs.

93 The National Child Care Management System is being implemented progressively across child care services from 1 July 2007 to 30 June 2009: Australian Government Department of Families, Community Services and Indigenous Affairs, *Child Care Management System* (2007) <www.facsia.gov.au/internet/facsinternet.nsf/childcare/ccms.htm> at 10 April 2008.

94 A policy for the disclosure of protected information relating to child care services was developed by the Department that previously regulated this area and is included each year in the *Child Care Service Handbook*: Department of Families, Community Services and Indigenous Affairs, *Child Care Service Handbook 2006–2007* (2007), App 1.

95 Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007.

96 National Children's and Youth Law Centre, *Submission PR 166*, 1 February 2007.

97 See Ch 3.

Identification in criminal matters and in court records

69.83 Information held by courts—including case files, judgments, and case management systems—often identify children and young people who are associated with proceedings, whether as a party to a civil or administrative proceeding, a defendant or victim in a criminal matter, a child involved in a family law dispute, a witness, or merely mentioned as part of the proceedings.

69.84 The judicial records of courts are presently exempt from the *Privacy Act*.[98] Courts traditionally have been responsible for governing access to these records, and policies vary from court to court. As noted in Chapter 11, however, the advent of online access to court records opens up the possibility of these records being readily viewed by a large number of people for a variety of purposes. Given the extent of personal information that may be contained in court records, this raises significant privacy concerns.

69.85 The privacy of children and young people inside the courtroom has attracted more judicial and legislative protection than the privacy of children in other circumstances.[99] Both the United Nations Convention on the Rights of the Child (CROC) and the *United Nations Standard Minimum Rules for the Administration of Juvenile Justice 1985* (the Beijing Rules) refer specifically to a young person's right to privacy at all stages of juvenile justice proceedings.[100] Rule 8.1 of the Beijing Rules notes that this is 'in order to avoid harm being caused to her or him by undue publicity or by the process of labelling'. The rule is explained in the official commentary.

> Young persons are particularly susceptible to stigmatization. Criminological research into labelling processes has provided evidence of the detrimental effects (of different kinds) resulting from the permanent identification of young persons as 'delinquent' or 'criminal'. Rule 8 also stresses the importance of protecting the juvenile from the adverse effects that may result from the publication in the mass media of information about the case (for example, the names of young offenders, alleged or convicted).[101]

69.86 Concerns also have been raised about the psychological damage that a child or young person involved in, or associated with, other kinds of cases might experience if identified in the media. This could include particularly difficult family law cases, child welfare cases, or high profile criminal law cases where the defendant has children who might suffer as a result of publication of the name or image of the accused.[102] Stigma

---

98 The ALRC does not recommend any change to this situation: see discussion in Ch 35.

99 J Moriarty, 'Children, Privacy and the Press' (1997) 9 *Child and Family Law Quarterly* 217, 219.

100 *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990), art 40(2)(b)(vii); *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985), r 8.1. See Ch 68 for a discussion of the application of these international instruments in Australia.

101 *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985), r 8 commentary.

102 See, eg, R Taylor, 'Re S (A Child) (Identification: Restrictions of Publication) and A Local Authority v W: Children's Privacy and Press Freedom in Criminal Cases' (2006) 18 *Child and Family Law Quarterly* 269.

also may attach, for example, to immigration cases involving refusal of visas or applications for government payments.[103]

69.87 Based on the fundamental rule that proceedings generally take place in open court, the common law has developed principles regarding a court's power to suppress publication of certain details of evidence before the court, balancing certain public interests against the interests of open justice. One such public interest includes protecting the interests of children.[104] Many Australian courts and tribunals have specific powers to make suppression orders under their establishing legislation.[105]

69.88 Legislation relating to child welfare and criminal matters before children's courts in most jurisdictions have prohibitions on the publication of identifying information about a child who is involved in proceedings.[106] The *Family Law Act* has a more general prohibition in relation to any person who is a party, related to or associated with a party, or is a witness to proceedings.[107] The extent of the prohibitions vary, and in most cases the legislation permits, or a judge may permit, publication in certain circumstances.[108] One exception is the Northern Territory legislation relating to juvenile offenders, which has as its starting point that there is no prohibition on publication, but gives the court a discretion to order that a report, information relating to proceedings or the results of proceedings, not be publicised.[109]

Submissions and consultations

69.89 While the NCYLC suggested it may be appropriate to move child welfare and criminal law privacy-related provisions into the *Privacy Act*,[110] there was support for

---

103 For example, the case of *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83 involved a rejected application for Austudy at the student homeless rate, including addresses and details of the applicant's relationship with his parents. Note that *Migration Act 1958* (Cth) s 91X prohibits the publication of names of applicants for protection visas in the High Court of Australia, Federal Court of Australia or Federal Magistrates Court.

104 *Johnston v Cameron* (2002) 124 FCR 160, 167. It should be noted that in the United Kingdom, following the introduction of the *Human Rights Act 1998* (UK), much of the debate is now centred around competing rights such as the right to privacy versus the freedom of expression: H Fenwick, 'Clashing Rights, the Welfare of the Child and the Human Rights Act' (2004) 67 *Modern Law Review* 889; I Cram, 'Minors' Privacy, Free Speech and the Courts' (1997) *Public Law* 410.

105 See, eg, *Federal Court of Australia Act 1976* (Cth) s 50; *Administrative Appeals Tribunal Act 1975* (Cth) s 35(2).

106 See, eg, *Children and Young Persons (Care and Protection) Act 1998* (NSW) s 105; *Children (Criminal Proceedings) Act 1987* (NSW) s 11. The relevant provision of the *Children (Criminal Proceedings) Act 1987* (NSW) is the subject of a current inquiry by the New South Wales Legislative Council Standing Committee on Law and Justice.

107 *Family Law Act 1975* (Cth) s 121.

108 See, eg, the power of the court to order that the name and identity of certain young convicted offenders be made public in *Juvenile Justice Act 1992* (Qld) s 234.

109 *Youth Justice Act 2005* (NT) s 50. See also discussion of a number of examples of media reporting in the Northern Territory in ABC Radio National, 'Naming and Shaming Juvenile Offenders', *Law Report*, 3 October 2006.

110 National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.

retaining the purpose-built provisions preventing the disclosure of the identity of a child or young person in relation to juvenile justice proceedings in the specific legislation in each jurisdiction.[111] The absence of such a provision in the Northern Territory, however, was seen as requiring specific reform.[112]

69.90 Some young people allegedly involved in criminal behaviour were named, or publicly identified through publication of their photograph, in the media following the Cronulla riots in December 2005.[113] It was suggested in a number of submissions that the provisions that restrict disclosure of the identity of children and young people should be extended to cover criminal investigations as well as court proceedings, because the policy reasons for this protection apply at all stages of the criminal process.[114]

69.91 The ALRC did not receive any submissions suggesting there were problems with the handling of court records involving children and young people, with the exception of one stakeholder concerned about the operation of the spent convictions scheme in relation to young offenders, and the privacy concerns arising from this issue.[115] Broader issues regarding privacy of court records are discussed in Chapters 11 and 35.

ALRC's view

69.92 In this Report and *Same Crime, Same Time: Sentencing of Federal Offenders* (ALRC 103),[116] the ALRC has noted the public policy reasons behind prohibiting the public identification of young people involved in criminal proceedings—especially the rehabilitative aims of the juvenile justice system. It is of particular concern that the Northern Territory has no automatic limitation on publication of court proceedings that identify a young person. In ALRC 103, the ALRC recommended the enactment of a provision prohibiting the publication of a report of criminal proceedings that identifies, or is likely to lead to the identification of, a child or young person.[117] Such a prohibition is appropriate. The Australian Government should implement this recommendation.

---

111 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

112 National Children's and Youth Law Centre, *Submission PR 166*, 1 February 2007.

113 Ibid, NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

114 Youthlaw, *Submission PR 390*, 6 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007; National Children's and Youth Law Centre, *Submission PR 166*, 1 February 2007; Youthlaw, *Submission PR 152*, 30 January 2007; NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007. See also concerns about case naming a 12 year old pregnant girl (ie, a victim) in the media where no charges were laid: J Simpson, *Submission PR 336*, 29 October 2007.

115 Youthlaw, *Submission PR 390*, 6 December 2007.

116 Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), [27.62]–[27.66].

117 Ibid, Rec 27–1. Due to the scope of the terms of reference of that inquiry, the recommendation was limited in application to the sentencing, administration and release of federal offenders.

69.93 The ALRC also encourages consideration of broader provisions relating to public identification of a child or young person alleged to have committed a crime, applying throughout the criminal investigation and proceedings. The ALRC considers that these provisions are situated most appropriately in relevant state and federal legislation dealing with child welfare or criminal matters. This issue lies beyond the scope of this Inquiry and the ALRC has not made a recommendation on the issue.

69.94 While issues relating to spent convictions schemes are outside the scope of this Inquiry, the ALRC notes that the development of uniform spent conviction laws are currently under consideration by the Standing Committee of Attorneys-General (SCAG).[118]

Family law

69.95 Children and young people are often involved in counselling or family dispute resolution services undertaken as part of a family law matter. Counselling and family dispute resolution services in association with family law disputes are now offered by private sector services (including not-for-profit services) which, unless they fall within an exemption, are subject to the NPPs.[119] The *Family Law Act 1975* (Cth) includes provisions governing the confidentiality of such services.[120] While an adult can give permission to have his or her information disclosed for any purpose, information provided by an individual under the age of 18 can be disclosed only with the agreement of each of the persons with parental responsibility for the child, or the approval of the court.[121]

Submissions and consultations

69.96 Generally, submissions and consultations did not raise any issues of concern about the operation of the *Family Law Act* or the privacy policies in operation in the Family Court of Australia, the Family Court of Western Australia or the Federal Magistrates Court.

69.97 The exception was the NCYLC, which submitted that the operation of ss 10D(3) and 10H(3) of the *Family Law Act*—which provide that information about a child may be disclosed if each of the persons with parental responsibility for the child agrees—operate contrary to the rights-based approach in the *Privacy Act* by excluding the involvement of the child in the decision-making process.[122] The NCYLC indicated it

---

118 Standing Committee of Attorneys-General, 'Communiqué' (Press Release, 28 March 2008).

119 Until 1 July 2006, confidential counselling and family dispute resolution services were also provided by specialised staff of the Family Court of Australia who were subject to the IPPs. These staff are now called 'family consultants' and no longer provide confidential services.

120 *Family Law Act 1975* (Cth) ss 10D, 10H. These provisions became operational on 1 July 2006.

121 Ibid ss 10D(3), 10H(3).

122 National Children's and Youth Law Centre, *Submission PR 166*, 1 February 2007.

had broader concerns about the lack of provision for the rights of children to be involved in family law dispute resolution processes generally.[123]

ALRC's view

69.98 The ALRC agrees that ss 10D(3) and 10H(3) of the *Family Law Act* are not consistent with the recommended approach under the *Privacy Act* and the general principles of involvement of children and young people in decision-making processes as set out in CROC. These provisions should be reviewed, giving consideration to an improved process for involving a child or young person in the decision.

69.99 From a privacy perspective, and consistent with the ALRC's recommendations in Chapter 68, it would be appropriate to amend the provisions to require the consent of a child or young person with decision-making capacity to the disclosure of his or her personal information. Due to the contexts in which ss 10D(3) and 10H(3) may operate, it may be appropriate to apply the ALRC's recommended age of presumption of capacity and require consent to disclosure from a young person aged 15 or over.

69.100 The ALRC is concerned, however, that there may be issues additional to privacy concerns that affect the operation of ss 10D(3) and 10H(3). The focus of this Inquiry is on privacy. The ALRC has not had an opportunity to identify and give full consideration to those additional issues, and therefore no recommendation is made for amendment to the *Family Law Act*. The ALRC suggests that appropriate consideration should be given to an amendment by the Attorney-General's Department, which has responsibility for the *Family Law Act*. Alternatively, it may be appropriate that the Family Law Council[124] give further consideration to the issue.

69.101 The broader issue of child-inclusive practices in family dispute resolution is well outside the scope of the this Inquiry. The ALRC notes, however, that there are models for child-inclusive practices in family dispute resolution, and that these are steadily gaining favour in Australia.[125]

Child welfare and juvenile justice

69.102 Child welfare and juvenile justice jurisdictions are the responsibility of the states and territories under existing federal arrangements. Children and young people who come into contact with either the child welfare or juvenile justice systems often have large amounts of personal information collected about them, much of it of a

123 National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.

124 The Family Law Council is a statutory authority established under the *Family Law Act 1975* (Cth). The Council's functions are to advise and make recommendations to the Attorney-General concerning family law.

125 L Moloney, 'Child-Sensitive Practices in High-Conflict Parenting Disputes: A 30-Year Road to Serious Reform' (2006) 12 *Journal of Family Studies* 37; L Moloney and J McIntosh, 'Child-Responsive Practices in Australian Family Law: Past Problems and Future Directions' (2004) 10 *Journal of Family Studies* 71.

sensitive nature. Legislation in each jurisdiction deals with the handling of records in that jurisdiction containing personal information of children and young people.[126]

69.103 A privacy-related issue that has arisen in the area of child welfare is the sharing of information between agencies where the safety of children and young people is at issue—for example, where there is evidence that the child may be at risk of physical or sexual abuse. All states and territories have laws in place that, in practice, provide exceptions to privacy laws by allowing or requiring disclosure of personal information in certain circumstances. A number of bodies, however, have identified instances where a child has been seriously injured or killed by a parent where disclosure of information about the parent's behaviour to appropriate service providers could have helped to prevent the injury or death.[127]

69.104 The ALRC did not receive any submissions raising specific concerns about the handling of child welfare or juvenile justice records. Issues surrounding the sharing of information in appropriate circumstances were, however, raised as matters of general concern.

ALRC's view

69.105 The issue of sharing information in child welfare and other contexts is considered in Chapter 14. The 'Use and Disclosure' principle, as discussed in Chapter 25, seeks to improve the balance between the need for information sharing in child protection contexts and maintaining an appropriate level of privacy protection. In particular, the ALRC has recommended removing the imminency requirement from the exception to the principle, allowing disclosure where necessary to lessen or prevent a serious threat to an individual's life, health or safety without having to prove that the threat was imminent.[128] The recommended changes to the 'Use and Disclosure' principle, together with improved clarity of privacy laws generally and better information sharing practices, should alleviate many of the concerns raised in this context by removing legal and practical barriers to the release of personal information in appropriate situations.

---

126 See, eg, *Children and Young Persons (Care and Protection) Act 1998* (NSW); *Juvenile Justice Act 1992* (Qld).

127 New South Wales Ombudsman, *Report of Reviewable Deaths in 2004* (2005); Child Death Review Team, *Fatal Assault of Children and Young People: Fact Sheet* (2003) New South Wales Commission for Children and Young People; Community Services Ministers' Advisory Council, *Submission PR 47*, 28 July 2006.

128 See Rec 25–3.

Taking photographs and other images

Background

69.106 The taking of photographs and other images of children and young people without consent has raised significant concerns in recent times. While the issues are not limited to photographs and images of children and young people, recent controversies have included: the taking of photographs of young male rowers and footballers and posting them on a website containing links to what the media described as a 'gay website'; discovery of a website containing hundreds of images of children taken at recreational sites in Queensland, and thought to be used for sexual gratification; and examples of 'upskirting'—the covert taking of photographs underneath clothing—in a number of public places.[129]

69.107 Mobile phone cameras and mobile phone video cameras appear to have heightened these concerns, due to their small size and availability. The issue of unauthorised taking of images, however, extends beyond any one type of technology. One author has noted that concerns about covert taking of photographs have existed since the 1890s, and have reappeared on a regular basis as different forms of cameras became available.[130] Most recently, the concerns about unauthorised images have exploded with the ease and accessibility of online publication.

69.108 Community concerns led SCAG to consider the issue. A discussion paper released for public comment in August 2005 set out the concerns and raised a number of options for reform.[131] While the paper was particularly focused on the posting of unauthorised photographs on the internet, much of the discussion addressed the issue of taking photographs generally. The SCAG discussion paper includes extensive comment on the issue of giving consent to the taking of a photograph. The discussion paper notes that the absence of consent may affect whether the taking of a photograph is considered to be unauthorised and, if consent was obtained, whether the subsequent use is connected with any consent that was given at the time the photograph was taken.[132]

---

129 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005), 5.

130 C Ludlow, '"The Gentlest of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135, 137. See also Australian Mobile Telecommunications Association, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, October 2005. The seminal article on privacy was prompted by advances in photographic technology: S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

131 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005). For an overview of some of the examples that have led to consideration of the issue, see [7]–[18].

132 See, eg, Ibid, [31]–[38]. Some jurisdictions were pushing for uniform criminal laws on these issues through SCAG, although the issue was not discussed at the March 2008 meeting: see K Ngyuen, 'Law Chiefs have their Eyes on Voyeurs', *The Age* (online), 28 July 2006, <www.theage.com.au> and Standing Committee of Attorneys-General, 'Communiqué' (Press Release, 28 March 2008).

69.109 The Victorian Law Reform Commission (VLRC) also has commenced an inquiry on surveillance in public places. It is expected that a number of issues concerning the taking and use of unauthorised photographs will arise in that inquiry. The VLRC is planning to release a consultation paper later in 2008.

The *Privacy Act* and images

69.110 The *Privacy Act* protects personal information that is held, or collected for inclusion, in a 'record'. A 'record' is defined to include a photograph or other pictorial representation of a person.[133] If an individual's identity is apparent, or can reasonably be ascertained, from a photograph or other image, then the collection, use and disclosure of that image is covered by the *Privacy Act*. This extends to video images as well as still photographs. The rest of this chapter uses the term 'image' to cover photographs and moving images. All of the privacy principles applicable to the collection and use and disclosure of personal information also will apply to the taking and publication of images.

69.111 As with other forms of personal information, the coverage of images is limited by the scope of the *Privacy Act*. For example, an image is not covered by the *Privacy Act* if it was taken by an individual who is acting in their private capacity. The image is also not covered if the image was taken by someone acting on behalf of a small business.[134] Similarly, images taken by a person acting on behalf of a state or territory agency are not covered by the *Privacy Act*, although they may be covered by a state or territory law.[135]

Submissions and consultations

69.112 A number of stakeholders raised concerns about the lack of clarity of the existing law in relation to photographing children. Some expressed particular concern about the ease of taking and disseminating photographic images using mobile or digital technology.[136]

69.113 Stakeholders highlighted the need to safeguard the safety and privacy of children from people with no legitimate purpose for taking and publishing photos.[137] The ALRC was presented with evidence about the harm that can be done to children where they are the victims of using photographs for sexual gratification, even where

---

133 *Privacy Act 1988* (Cth) s 6. For more detailed discussion of the definitions of 'record' and 'personal information', see Ch 6.

134 Although see Rec 39–1 which seeks to bring small business under the coverage of the *Privacy Act*.

135 See Ch 2 for an overview of applicable state and territory privacy laws and the ALRC's recommendations in Ch 3 for introduction of nationally consistent privacy laws.

136 See, eg, Youth Affairs Council of Victoria Inc, *Submission PR 172*, 5 February 2007.

137 Queensland Police Service, *Submission PR 222*, 9 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

the photograph itself was not sexually explicit in nature.[138] The Queensland Commission for Children and Young People and Child Guardian indicated that it regularly receives phone calls from concerned parents, managers of sporting associations, and others who believe it is against the law to take photos of children at events.[139] One stakeholder lamented that this is the 're-engineering of society by stealth and misinformation'.[140] The OPC considered that developing social protocols that make it acceptable to ask a person to refrain from using a camera on a beach or outside of a school is a positive step.[141]

69.114 The issues around unauthorised images are not limited to safety concerns about children and young people. As noted in Chapter 67, the ALRC's consultations with young people indicated that the online publication of images without the consent of the subject of the photograph is a common occurrence—whether or not the image itself was taken with the subject's consent. The online posting itself was taken for granted by some, and the ease of online publication accepted as a reality by most. While the posting may not be criminal in nature, the possible consequences of unauthorised posting can include bullying, ridicule, embarrassment and generally an invasion of privacy.

69.115 Overall, concerns about taking and using unauthorised images, particularly of children, led some to consider the need for stricter regulation.

> Sadly, there is now good reason for the existence of clear guidance through the *Privacy Act* governing limitations on the broadcasting of identifying images of children, restricting the ability of organisations to publicly display a photo of a child in their care, without the express consent of the parent or guardian.[142]

69.116 Generally, however, there was not widespread support for a blanket ban on the taking of images of children without express consent. Instead, there were calls for a clearer regime which balances sensibly the need to protect children from exploitation for sexual and commercial purposes with the need not to place undue restrictions on the taking of images by parents, family and friends.[143] While there are some individuals who offend others through inappropriate behaviour, these are in the minority and the vast majority of appropriate users should not be restricted from using

---

138 Queensland Police Service, *Submission PR 222,* 9 March 2007.

139 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

140 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

141 Office of the Privacy Commissioner, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Use of Photographs on the Internet and Related Privacy Issues,* November 2005.

142 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

143 Queensland Police Service, *Submission PR 222,* 9 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

photography in appropriate ways.[144] Some considered that privacy laws are an appropriate method for regulating this issue.[145]

69.117 In contrast, the Arts Law Centre of Australia was opposed to any law which requires photographers or documentary filmmakers to obtain the consent of individuals before taking a photograph or film footage.[146] The concerns of the artistic community in relation to privacy laws preventing street art and the taking of photographs in public places are addressed in more detail in Chapter 74.

Options for reform

69.118 In the SCAG discussion paper on unauthorised photographs, a number of reform options were discussed, including:

- possible criminal offences regarding unauthorised use of photographs of children;
- possible civil remedies regarding unauthorised publication of images of people;
- 'take down' provisions for online content; and
- education campaigns.

Criminal offences

69.119 There are a number of existing criminal laws that address the taking and use of unauthorised images for offensive purposes. Some of these include:

---

144 Australian Mobile Telecommunications Association, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, October 2005.

145 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171*, 5 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

146 Arts Law Centre of Australia, *Submission PR 125*, 15 January 2007. See also Australian Library and Information Association, *Submission PR 446*, 10 December 2007; Australian Network for Art and Technology, *Submission PR 434*, 10 December 2007; National Association for the Visual Arts Ltd, *Submission PR 415*, 7 December 2007; P Hammer, *Submission PR 396*, 7 December 2007; N Griffiths, *Submission PR 395*, 7 December 2007; Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007; R Anderson, *Submission PR 373*, 4 December 2007; E Halvorson, *Submission PR 367*, 3 December 2007; M Schaefer, *Submission PR 364*, 3 December 2007; O Esmonde-Morgan, *Submission PR 361*, 3 December 2007; H Page, *Submission PR 360*, 2 December 2007; K Purcell, *Submission PR 359*, 2 December 2007; J Mortelliti, *Submission PR 357*, 2 December 2007; National Association for the Visual Arts, *Submission PR 151*, 30 January 2007.

- use of surveillance devices to record a 'private activity' without consent;[147]
- filming for indecent purposes;[148]
- making an image of a child engaged in a private act for prurient purposes;[149]
- making indecent visual images of a child under the age of 16;[150]
- committing indecent or offensive acts in a public place;[151]
- child pornography offences;[152] and
- using a telecommunications network or carriage service to facilitate certain offences.[153]

69.120 As noted in the SCAG discussion paper, a number of situations of concern do not fit neatly into the existing laws. Most of the existing criminal offences involve elements of 'private activity' or a 'private act', so that any activity carried out in a public environment, or at least an activity in a place where privacy is not expected—such as rowing, swimming or playing in a public playground—is not covered by the particular offence. To deal with particular concerns about 'upskirting', Victoria has introduced specific offences for the act of deliberately observing or capturing images of the anal or genital area of someone without their knowledge and in circumstances where it would be reasonable to expect that they would not be photographed in this way.[154] It is also an offence intentionally to distribute such images without the person's consent. There is, however, a question of whether criminal offences should more broadly extend to the making of images without consent in any public or private

---

147 See, eg, *Surveillance Devices Act 1999* (Vic) ss 6–7; *Surveillance Devices Act 2000* (NT) s 5; *Surveillance Devices Act 1998* (WA) ss 5–6. Not all of the surveillance devices legislation in Australia, however, has a general prohibition on the use of surveillance devices without authorisation or consent: see, eg, in South Australia the prohibition is limited to listening devices: *Listening and Surveillance Devices Act 1972* (SA) s 4.

148 See, eg, *Summary Offences Act 1988* (NSW) pt 3B. In some jurisdictions, however, the offence only applies where the indecent material is produced for the purpose of sale: see, eg, *Summary Offences Act 1953* (Qld) pt 7.

149 See, eg, *Criminal Law Consolidation Act 1935* (SA) s 63B.

150 See, eg, *Criminal Code* (Qld) s 210(1)(f)

151 See, eg, Ibid s 227(1); *Summary Offences Act 1988* (NSW) s 4; *Police Offences Act 1935* (Tas) s 13.

152 See, eg, *Crimes Act 1958* (Vic) pt 1 div 13; *Criminal Code Act 1924* (Tas) ss 130–130G.

153 See, eg, *Criminal Code* (Cth) s 474.14 (using a telecommunications network to commit a serious offence); s 474.17 (using a carriage service to menace, harass or cause offence); ss 474.19–474.20 (using a carriage service to intentionally access, transmit or make available child pornography material); ss 474.22–474.23 (using a carriage service to intentionally access, transmit or make available child abuse material).

154 *Summary Offences Act 1966* (Vic) div 4A, inserted by the *Summary Offences Amendment (Upskirting) Act 2007* (Vic). Similar offences have been introduced to the South Australian Parliament for debate: Summary Offences (Indecent Filming) Amendment Bill 2008 (SA).

situation where the purpose for making the image is to provide for sexual arousal or sexual gratification.

69.121 Another concern raised with the Inquiry is that a number of the criminal offences in the states and territories do not cover images of children that are not sexually explicit in nature, but that may be used for purposes of sexual gratification. The Queensland Police Service provided the ALRC with a number of case studies involving images of children, in socially appropriate situations and attire, which had been taken and used for sexual gratification.[155] Due to the existing definitions of 'child exploitation material', 'child abuse material' and 'child pornography' material in Commonwealth and Queensland legislation, the Police have had only limited success in prosecuting the individuals involved, and even greater difficulties in having the images removed from the internet as they were not considered to be offensive content.

Civil rights and remedies

69.122 There are valid concerns that there are some types of capture and publication of images which may not be criminal in nature, but still affect an individual's privacy interests.

69.123 The SCAG discussion paper looked at the use of copyright law enacted in the Netherlands to eradicate the trade in video recordings showing children on beaches and nudist beaches where the recording is made without the parents' or child's consent.[156] As part of the civil response to the issue, the *Copyright Act 1912* (the Netherlands) was amended to provide that the publication of a photographic or video portrait made without a commission is not permitted if this would be contrary to the reasonable interests of the person shown in the photograph or video. The Act provides that a child or his or her legal representative may apply to the courts for an injunction to restrain publication. A number of submissions made in response to the SCAG discussion paper supported this kind of 'reasonable interests' approach, but questioned whether amendment to Australian copyright law was the best response.[157]

Take down notices for online content

69.124 The current take-down notice scheme administered by the Australian Communications and Media Authority (ACMA) for the regulation of internet content is dependent on the *National Classification Code* and decisions of the Classification Board to determine what is prohibited content that can be the subject of a take-down

---

155 Queensland Police Service, *Submission PR 222*, 9 March 2007.

156 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005) citing *Convention on the Rights of the Child: Initial Reports of States Parties Due in 1997: Netherlands: Addendum*, CRC/C/51/Add.1 (1997).

157 See, eg, New South Wales Commission for Children and Young People, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Use of Photographs on the Internet and Ancillary Privacy Issues*, October 2005.

notice.[158] Prohibited content includes material rated, or likely to be rated, RC or X18+, or material of a R18+ or MA15+ rating where access is not restricted appropriately. There is no specific regulation in Australia of internet content that is an invasion of an individual's privacy.

Conditional rights

69.125 Many bodies have begun to include as part of conditions of entry to premises, or participation in an event, that cameras, video cameras or mobile phones incorporating cameras or video cameras, are not to be brought onto the premises or used. This has become typical in change rooms and private gyms, where people expect an element of privacy, but has been more controversial when applied to public events and places such as life saving and sports carnivals, or public swimming pools.[159]

Education

69.126 The activity of taking images appears to many members of the community to be under siege. The ALRC heard complaints from people who were challenged or castigated when taking photographs of family members, and from those concerned about a loss of artistic freedom. Conversely, others have concerns about guaranteeing the privacy and safety of children in the community. Clearly there is confusion about what is acceptable, what is legal, and when inappropriate behaviour can be stopped or punished. It is also an area where community attitudes and behaviours are changing.

69.127 A number of bodies have begun to publish educational information about the law surrounding the taking of images in public. The Privacy Commissioner of Victoria has published a fact sheet on mobile phones containing cameras covering many of the issues of concern and the legal protections in place.[160] The Queensland Commissioner for Children and Young People and Child Guardian has developed a similar fact sheet on photography and video footage, with a particular emphasis on children's and young people's right to privacy.[161]

ALRC's view

69.128 The ALRC does not recommend a blanket ban on the taking of images without consent. This is not seen as a practical or desirable option. Decisions regarding imposing conditions of entry or participation that include a ban on taking images should be left to the bodies owning premises or organising events. These views were set out in DP 72.[162] The ALRC received no comment on this position.

---

158 *Broadcasting Services Act 1992* (Cth) sch 7.

159 R Grayson, 'No Right Not to Be Photographed—Councils Overreact', *On Line Opinion* (online), 12 July 2005, <www.onlineopinion.com.au>.

160 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras—Info Sheet 05.03* (2003).

161 Queensland Government Commission for Children and Young People and Child Guardian, *Tips for Parents on Photography of Children and Young People*, Fact Sheet 3 (2007).

162 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [59.112].

69.129 As noted above, however, there is confusion and concern around issues of taking and publishing images of children and young people. The ALRC believes that a multifaceted approach is required to alleviate these concerns.

69.130 The criminal law regulates more severe forms of inappropriate behaviour. It is clear that there are gaps in the existing criminal law, however, and not all inappropriate conduct relating to the taking and use of unauthorised images is presently covered in all jurisdictions. Further consideration must be given to what types of behaviour the community wants to label as criminal, but merely taking an image without consent should not be considered a criminal act.

69.131 It is outside the scope of this Inquiry to examine and improve criminal laws to ensure that the full range of inappropriate behaviour relating to the making and using of offensive images is dealt with effectively in criminal offences. This issue should be progressed further by SCAG to ensure uniformity across the jurisdictions. The ALRC notes, however, that stakeholders contributing to this Inquiry have not expressed support for making it a criminal offence to take an image of a child or an adult without consent. Any proposed criminal offences should not be unduly restrictive and must still provide for family, friends, community bodies, schools, media, the artistic community and others to take and publish acceptable images.

69.132 The ALRC's considerations have focused on privacy regulation that may assist with concerns in this area. While acknowledging that individuals taking and publishing images for personal use are not covered under the *Privacy Act*, the ALRC does not consider it appropriate to broaden the take-down notice scheme to address privacy issues arising from the online publication of personal information. As discussed in Chapter 11, a take-down notice scheme would require a decision-maker to balance the right of freedom of expression and the right to individual privacy. It is more appropriate for a court, rather than a regulator, to undertake such a balancing act. The ALRC also queries the utility of an Australian take-down notice scheme given the ease of moving internet content to a website hosted in another jurisdiction. The statutory cause of action for a serious invasion of privacy, recommended in Chapter 74, is a more appropriate approach to regulation of the issue. The issuing of a take-down notice may be an appropriate remedy for a court to order in certain cases.

69.133 The statutory cause of action will provide protection where a person (including a child or young person) has a reasonable expectation of privacy and the act or conduct is sufficiently serious to cause substantial offence to an ordinary person. This will provide a remedy in cases where there is serious harm arising from the invasion of privacy, and also provide a message to the community in general about what constitutes acceptable behaviour.

69.134 As discussed in Chapter 74, a statutory cause of action will balance the right of privacy with competing rights, in particular freedom of expression. Combined with

appropriate criminal offences to deal with the most unacceptable actions, a statutory cause of action allows a balanced way forward to allow individuals to continue to photograph and video friends and family, and to allow the artistic community to use this medium of artistic expression, while providing some limits on the invasion of personal privacy.

69.135 It is clear, however, that further information about the laws relating to the taking of images is required in order to educate the community, provide information on what is appropriate and inappropriate behaviour, inform the public about available remedies, and facilitate an informed debate about future law reform in this area. In conjunction with proposals for the introduction of a statutory cause of action for a serious invasion of privacy, the ALRC recommends that the OPC should provide information to the public concerning the statutory cause of action.[163] As the publication of images, particularly in the online environment, is an issue of particular concern to the community, such information should include discussion of when publication of an image is likely to be considered an invasion of privacy.

163 See Rec 74–7.

70. Third Party Representatives

Contents

Introduction

70.1 This chapter considers existing laws and practices applying to third parties that assist an individual to make decisions under the *Privacy Act 1988* (Cth), or make decisions on behalf of the individual. Individuals may require assistance from a third party because of a failing or fluctuating capacity to make decisions, possibly because of a disability, injury, illness or cognitive impairment. Third parties may also be required to facilitate communication for non-English speakers or persons with a communicative disability. Alternatively, allowing third parties to act on behalf of the individual may be a matter of convenience for the individual. The third parties involved may be carers, spouses, parents, adult children, interpreters, counsellors, legal representatives or any other person chosen by the individual. The arrangements may be temporary, one-off, short-term arrangements, or permanent.

70.2 Two decision-making situations are considered in this chapter: where the individual has limited or no capacity to make decisions, and a third party is required to

represent the individual; and where the individual provides consent for a third party to assist, or make the decision for, the individual.

70.3 Stakeholders highlighted numerous problems for individuals and their third party representatives in gaining access to benefits and services due to perceived or real conflicts with the *Privacy Act*. The ALRC has considered how the *Privacy Act* can be amended to give better recognition to third party representatives and facilitate improved interactions without leaving individuals at risk of abuse.

70.4 There does not appear to be any need to amend the *Privacy Act* to deal with issues concerning assessment of capacity, application of a presumption of capacity, or to ensure recognition of third parties who are authorised as substitute decision makers by another federal, state or territory law. The ALRC recognises that dealings with individuals under the *Privacy Act* are often only a part of the overall relationship between the individual and the agency or organisation, and should not be considered in isolation. Any attempt by the *Privacy Act* to impose specific provisions relating to capacity would add greater complexity to the already complicated operation of the often inconsistent state and territory guardianship and administration laws. In addition, the power for a third party authorised by another federal, state or territory law to act in place of the individual for the purposes of the *Privacy Act* is given by the relevant appointment or legislation.

70.5 The ALRC acknowledges, however, that problems can arise in practice when agencies and organisations subject to the *Privacy Act* deal with issues of capacity and the recognition of substitute decision makers authorised by another federal, state or territory law. The ALRC recommends that the Office of the Privacy Commissioner (OPC) should develop and publish guidance to assist agencies and organisations to understand the application to the *Privacy Act* of relevant guardianship and administration and power of attorney legislation. The ALRC also recommends that agencies and organisations, that regularly handle personal information about adults with an incapacity, ensure that relevant staff receive training on issues concerning capacity, and in recognising and verifying the authority of third party representatives.

70.6 The ALRC does not recommend that the *Privacy Act* give specific authority to informal representatives—such as carers and family members who are not otherwise authorised by another law to act as a substitute decision maker—to make decisions automatically on behalf of an individual with an incapacity. Such authority is provided for in Australian guardianship and administration regimes in limited circumstances, involving routine medical treatment. Providing such authority in the *Privacy Act* would expose individuals to an unacceptable risk of invasion of their privacy.

70.7 It is consistent with the operation of the *Privacy Act*, however, to give recognition to third parties acting with the consent of the individual. The ALRC recommends that the *Privacy Act* should be amended to give greater certainty to arrangements that allow a third party nominated by the individual to act on his or her behalf. A nominee would act as a substitute decision maker for the individual, and an

agency or organisation could deal with the nominee as if he or she were the individual for the purposes of the *Privacy Act*.

70.8 Key elements of the nominee arrangement should be incorporated into the *Privacy Act*. These arrangements should allow sufficient flexibility for each agency and organisation to develop administrative arrangements that are suitable for the context in which it operates. The ALRC recommends that the OPC develop and publish guidance on establishing and administering nominee arrangements. The ALRC also recommends that the OPC guidance cover other consensual third party arrangements that assist the individual to make and communicate privacy decisions, including the use of interpreters, counsellors, and legal representatives.

Third party decision making under the *Privacy Act*

70.9 As discussed in Chapter 1, the focus of the *Privacy Act* is the protection of the privacy of an individual's personal information. As such, all of the rights and entitlements embedded in the Act are connected with the individual, and in some cases require or enable the individual to give consent, request access or exercise a right. There is no explicit recognition in the Act of third parties acting on behalf of individuals.[1]

70.10 For situations where an individual merely requires assistance from a third party, but the third party must have access to personal information about the individual in order to provide the necessary assistance, the 'Use and Disclosure' principle recommended in this Report provides that an agency or organisation may disclose personal information to a third party with consent of the individual.[2]

70.11 It is possible for an individual to authorise a third party to act on his or her behalf. While this is not set out in the *Privacy Act*, the OPC has advised that there is nothing in the Act that prevents such an authorisation.[3] On its website, the OPC confirms that the *Privacy Act* does not prevent an agency or organisation from dealing with a third party authorised by an individual to act on his or her behalf.[4] The OPC goes on to note that organisations have a variety of procedures to ensure appropriate authorisation, including identity validation procedures. The OPC suggests that some organisations with existing customer verification procedures for telephone services may use such procedures for authorisation of third parties. The OPC also notes, however, that an organisation may decide that the circumstances and risk require a

---

1 The ALRC recommends, in Ch 8, that family members or legal representatives should be able to exercise certain rights on behalf of deceased individuals.

2 See Ch 25. This also is the case under the Information Privacy Principles and the National Privacy Principles.

3 Office of the Privacy Commissioner, *FAQs: Can I Authorise Someone to Act on My Behalf when Dealing with a Business?* <www.privacy.gov.au/faqs/ypr/q14.html> at 25 March 2008.

4 Ibid.

more robust authorisation process, such as the provision of written authorisation. Further guidance is not provided, although it is stated that the

> Privacy Commissioner would expect that if a customer was to follow the security and identification procedures an organisation uses in its ordinary dealings, and give their consent, a third party may be able to act on that customer's behalf.[5]

70.12 Consensual authorisation is not a viable option, however, when dealing with an individual who lacks the capacity to provide authorisation. The 'authorised by law' exception in a number of the existing Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) has been interpreted as allowing for recognition of substitute decision makers authorised by a federal, state or territory law.[6] This is simply an implicit recognition of the powers of authorised substitute decision makers that have been established by the relevant federal, state or territory legislation or the instrument or order of appointment.[7] The OPC has stated that a third party is able to exercise a right on behalf of an individual where a formal guardianship or administration order is in place, despite the absence of an express provision to that effect in the *Privacy Act*.[8]

Examples of existing third party arrangements

70.13 A number of agencies and organisations have adopted third party arrangements as part of their normal course of business which allow for ongoing recognition of an authorised third party. For example, Optus has a procedure for establishing a third party authority nominated by the account holder to act on his or her behalf. A nominated person can request, change and supply information regarding the account. A nominated person, however, cannot do anything that requires the account holder's signature or verbal electronic authorisation, including changing personal details or activating a new service.[9] Optus notes that, in some cases, third party access is the primary form of communication between Optus and the customer, especially for customers with a disability or those from a non-English speaking background.[10]

---

5 Ibid.

6 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 214–215.

7 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

8 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.

9 A full list of actions that cannot be undertaken by a nominated person are set out at Optus, *Personal—Mobile Account Access* <www.optus.com.au> at 25 March 2008 and Optus, *Small Business—Third Party Access* <www.optus.com.au> at 25 March 2008. Where a power of attorney is granted for general purposes, and the legal document establishing the power of attorney is sighted by an Optus customer service representative, the nominated person will have the same level of access to an account as the account holder.

10 Optus, *Personal—Mobile Account Access* <www.optus.com.au> at 25 March 2008; Optus, *Small Business—Third Party Access* <www.optus.com.au> at 25 March 2008.

70.14 Telstra also has a system for naming an 'authorised representative' who is able to access information about an account on behalf of the 'legal lessee'.[11] MBF Health has an option for nominating a person to undertake membership transactions, collect benefits, or both, on behalf of the primary member. The nominee has the same rights and obligations as the primary member, including access to the health information of all persons on the membership.[12]

70.15 Centrelink has nominee arrangements that are underpinned by legislation.[13] Individuals can nominate any third party to act on their behalf in one or more of the following ways: to make enquiries only; to receive payments (payment nominee); or to act and make changes generally (correspondence nominee). Forms and processes for nominee arrangements are also used by Centrelink to recognise persons authorised as a substitute decision maker by a federal, state or territory law. As at 20 July 2007, there were 347,047 nominee arrangements in place: 25,753 payment arrangements; 285,398 correspondence only arrangements; and 35,896 with both payments and correspondence arrangements in place. Only 4% of these reflected a court, tribunal or guardianship or administration order or a formal power of attorney arrangement.[14]

70.16 The Centrelink nominee arrangements have operated administratively in the past, although they were given a legislative basis in 2002. On the introduction of the provisions, the need for a legislative basis was explained as follows:

> The amendments relating to nominees form a part of the measures being undertaken to give effect to the Government's commitment to implement a simpler and more coherent social security system.
>
> Nominees are particularly relevant to youth allowance, age pension and disability support pension recipients who have difficulty managing their own financial affairs.
>
> Currently, the law only provides for a payment nominee and arrangements relating to correspondence are dealt with administratively. Similarly, the current law does not clearly set out the duties and obligations of nominees. With an ageing population the use of nominees is likely to increase so it is considered appropriate to address these issues now.[15]

---

11 Telstra, *Access for Everyone: Your A–Z Guide* (2006).

12 MBF Health, *Form: Partner Authority/Application for Legal Authority*.

13 *Social Security (Administration) Act 1999* (Cth) pt 3A, which was inserted by the *Family and Community Services Legislation Amendment (Budget Initiatives and Other Measures) Act 2002* (Cth).

14 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), [2.180]. These figures were given by Centrelink in evidence to the Committee.

15 Explanatory Memorandum, Family and Community Services Legislation Amendment (Budget Initiatives and Other Measures) Bill 2002 (Cth), i. It was suggested to this Inquiry, however, that a legislative basis is not necessary for the operation of nominee arrangements consistent with the *Privacy Act*: Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007.

70.17 Part 3A of the *Social Security (Administration) Act 1999* (Cth) provides the detail for the operation of the nominee arrangements, including the functions and responsibilities of nominees. In particular, the payment or correspondence nominee has a duty to act at all times in the best interests of the principal beneficiary.[16] There is also provision for the suspension or revocation of nominee appointments.[17]

70.18 Concerns were expressed in previous inquiries about the potential for abuse of nominee arrangements governed by Centrelink,[18] including: inadequate safeguards around the appointment of nominees; inadequate penalties for a breach of nominee obligations; and problems with identifying abuse. In its 2007 report, *Older People and the Law*, the House of Representative Standing Committee on Legal and Constitutional Affairs noted that most of the concerns raised with the Committee centred on payment nominee arrangements, which have a higher risk of financial abuse than correspondence-only arrangements. Centrelink indicated to the Committee that it does not have a set schedule to review nominee arrangements, but only a small number of instances of abuse had been brought to Centrelink's attention.[19]

Problems with the *Privacy Act*

Impeding access to benefits and services

70.19 Many examples of situations where third parties were denied access to the personal information of another individual or experienced difficulty in communicating with an agency or organisation because of actual or perceived conflict with the *Privacy Act* were brought to the ALRC's attention during the course of this Inquiry. These included:

- a person unable to assist a sick friend to make payments or defer payments on a phone service while the friend was in hospital;[20]
- a husband unable to book a service on a washing machine because it was purchased in the wife's name;[21]
- widows and widowers having difficulties in changing financial details on joint accounts with banking institutions;[22]

---

16 *Social Security (Administration) Act 1999* (Cth) s 123O.
17 Ibid s 123E.
18 S Ellison and others, *Access to Justice and Legal Needs: The Legal Needs of Older People in NSW* (2004) Law and Justice Foundation of New South Wales, 334–335; Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), [2.179]–[2.185].
19 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), [2.179]–[2.185].
20 K Bottomley, *Submission PR 10*, 1 May 2006.
21 R Minahan, *Submission PR 482*, 13 December 2007.
22 B Such, *Submission PR 71*, 2 January 2007.

- organisations refusing to accept a verbal authorisation of the individual to release personal information to lawyers, financial counsellors and interpreters;[23]

- a friend assisting an individual who speaks English as a second language, being denied access to personal information despite being in the same room as the consenting individual at the time a phone call was made;[24]

- a parent unable to access information about a telecommunications service provided to the teenage child, despite the parent having established and paid for the service;[25] and

- other third party assistants, including lawyers, financial counsellors and social workers, authorised to speak on behalf of the individual to negotiate suitable outcomes, but unable to access personal information about the individual.[26]

70.20 Similar concerns were raised in stakeholder forums conducted as part of the OPC review of the private sector provisions of the *Privacy Act* in 2005 (OPC Review).[27]

70.21 Concerns and complaints about the impact of the *Privacy Act* on the ability of domestic partners to assist each other with account facilitation and payments were also commonly received during the ALRC's National Privacy Phone-in held in June 2006.[28]

> Current privacy laws are so heavily weighted against information flow that it is difficult for a modern family to operate effectively. What is classed as protection to some, is a hindrance to others. As a married man with children the levels of frustration my wife and I incur when trying to make enquiries or to alter contracts for phones, electricity, etc or anything really is way over the top. The amount of paper work that organisations claim to need under the umbrella of privacy is extreme. The number of times I am asked to put my wife on the phone or vice versa is an insult to us and hits at our own integrity … Privacy laws need to have some way of lifting all the restrictions married couples etc have to incur. It is not good enough to have a system where there are provisions for heaps of paperwork to be prepared. We are a family and should be treated as such.[29]

---

23 Legal Aid Queensland, *Submission PR 212*, 27 February 2007.
24 Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.
25 P Smart, *Submission PR 323*, 23 September 2007.
26 Legal Aid Queensland, *Submission PR 212*, 27 February 2007.
27 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.
28 The National Privacy Phone-in is described in more detail in Ch 1.
29 *ALRC National Privacy Phone-in*, June 2006, Comment #778.

70.22 A number of the concerns raised above could have been facilitated, consistently with the *Privacy Act*, if the agency or organisation had a process in place to obtain the consent of the individual whose personal information was in issue.

Vulnerable adults

70.23 General concerns were raised in submissions to this Inquiry about the balance between protecting vulnerable adults from unnecessary interference with their privacy and ensuring that they gain access to required services and benefits.[30]

> The particular circumstances of people with a decision-making disability can mean that many aspects of their lives are unnecessarily exposed to others, and their privacy is compromised. However, it is important that protection of privacy does not have an undesired effect of creating further barriers to necessary service provision, which would result in poorer outcomes and reduced quality of life for the individuals concerned.[31]

70.24 An important practical issue raised in submissions was the need to ensure that privacy legislation enables appropriate third parties to act on behalf of those who cannot act for themselves. An incapacity may be temporary or permanent, and can be caused by many different circumstances, including disability, injury, illness or cognitive impairment. It was suggested that there are inadequate alternative decision-making mechanisms in the *Privacy Act* to facilitate an exchange of information where an individual is unable to provide consent.[32]

70.25 In 2003–04, the Australian Guardianship and Administration Committee (AGAC) undertook a small survey designed to determine whether there have been any unanticipated adverse consequences as a result of privacy legislation for people who have a decision-making disability. While finding that the legislation generally worked well, the AGAC concluded that there was 'significant room for improvement in how a range of service providers interpret and apply the legislation in cases involving people who have a decision-making disability and their family members and allies'.[33] The AGAC speculated that problems arise primarily because organisations, in an attempt to comply with the *Privacy Act*, require individuals expressly to authorise another person to transact business on their behalf—something that cannot be done if the individual does not have capacity.

---

30 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007; Community Services Ministers' Advisory Council, *Submission PR 47*, 28 July 2006.

31 Government of South Australia, *Submission PR 187*, 12 February 2007.

32 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; National E-health Transition Authority, *Submission PR 145*, 29 January 2007.

33 Australian Guardianship and Administration Committee, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004. The AGAC reiterated these views in a submission to this Inquiry: Australian Guardianship and Administration Committee, *Submission PR 129*, 17 January 2007.

70.26 Concerns have been raised that, even in situations where a formal arrangement, such as an enduring power of attorney or a guardianship or administration order, is in place, these orders are not always respected.[34] While there is no provision in the *Privacy Act* that would prevent these transactions from proceeding, often in practice the formal arrangements are not recognised.

70.27 In *Older People and the Law*, the House of Representative Standing Committee on Legal and Constitutional Affairs considered substitute decision-making laws and practices on a national basis.[35] It recognised that the 'patchwork' of legislation on powers of attorney and, more generally, guardianship and administration legislation, leads to confusion about requirements for signing, registering, executing and recognising powers of attorney—particularly across state boundaries. It noted that the Department of Health and Ageing, through the Australian Health Ministers' Conference, is seeking to develop a nationally coordinated approach across a range of substitute decision-making mechanisms, including guardianship, advance care planning and wills.[36] The Committee considered that further work was required; and recommended that the Standing Committee of Attorneys-General (SCAG) work towards the implementation of uniform legislation on powers of attorney, and on guardianship and administration, in all states and territories.[37] Other issues considered by the Committee that would improve existing laws and practices for substitute decision making included the development:

- of campaigns to promote awareness of powers of attorney and their advantages, and better information strategies to inform principals of the implications of making a power of attorney, and attorneys of their responsibilities;[38]
- and implementation by SCAG and the Standing Committee of Health Ministers of a nationally consistent approach to the assessment of capacity;[39] and
- by SCAG of a national register of enduring powers of attorney.[40]

70.28 Problems for carers are most acute where there are informal arrangements in place for making decisions on behalf of an adult. This occurs where a family member, carer or friend makes decisions or assists in decision making without formal authority

---

34 K Bottomley, *Submission PR 10*, 1 May 2006. This concern was also identified by a number of callers to the ALRC National Privacy Phone-In.

35 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), Ch 3.

36 Ibid, [3.30].

37 Ibid, rec 16 in relation to powers of attorney legislation; rec 28 in relation to guardianship and administration legislation.

38 Ibid, rec 18.

39 Ibid, rec 19.

40 Ibid, rec 20.

provided by an instrument such as an enduring power of attorney, or appointment as a guardian or administrator by a tribunal, board or court. The existence of informal arrangements is consistent with the philosophy underpinning Australian guardianship and administration legislation, which seeks to maximise involvement in decision making by the individual and ensure that the least restrictive decision-making processes are available. Formal guardianship or administration orders are made as a last resort where informal arrangements have broken down.[41] Many service providers, however, will deal with third parties only where formal authorisation is provided. While the aim of the service providers is to protect the personal information of individuals, this practice may, as has been illustrated above, create problems for those individuals who need third party assistance to gain access to necessary services and benefits.

Adults with a temporary or permanent incapacity

Presuming capacity

70.29 The common law recognises—as a 'long cherished' right—that all adults must be presumed to have capacity until the contrary is proved. Where capacity is contested at law, the burden of proof lies with the person asserting the incapacity.[42]

70.30 A clear legislative statement on the presumption of capacity has been incorporated into guardianship and administration legislation in some jurisdictions. The Queensland legislation has the simple statement, included in the principles that apply across the Act, that 'An adult is presumed to have capacity for a matter'.[43] The Western Australian provision is more complex:

> Every person shall be presumed to be capable of —
>
> (i) looking after his own health and safety;
>
> (ii) making reasonable judgments in respect of matters relating to his person;
>
> (iii) managing his own affairs; and
>
> (iv) making reasonable judgments in respect of matters relating to his estate, until the contrary is proved to the satisfaction of the State Administrative Tribunal.[44]

70.31 In a recent discussion paper on capacity, the New South Wales (NSW) Attorney General's Department asked for feedback on whether it was necessary to include the

---

41 Legal Aid Queensland, *Submission PR 212*, 27 February 2007; Australian Guardianship and Administration Committee, *Submission PR 129*, 17 January 2007.

42 *Masterman-Lister v Brutton & Co* [2003] 3 All ER 162, 169; *L v Human Rights and Equal Opportunity Commission* (2006) 233 ALR 432.

43 *Guardianship and Administration Act 2000* (Qld) sch 1, pt 1. See also s 7(a). This is similar to the relevant United Kingdom legislation which states that 'A person must be assumed to have capacity unless it is established that he lacks capacity': *Mental Capacity Act 2005* (UK) s 1(2).

44 *Guardianship and Administration Act 1990* (WA) s 4(2)(b).

presumption in legislation.[45] A number of submissions in response to that discussion paper supported the inclusion of a decision-specific presumption of capacity in all relevant guardianship-related legislation in NSW.[46]

70.32 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC asked whether the *Privacy Act* should be amended to include a presumption of capacity.[47]

Submissions and consultations

70.33 There were mixed views expressed in submissions on whether a presumption of capacity should be incorporated into the *Privacy Act*. A number of stakeholders supported a legislative provision in order to clarify in the *Privacy Act* the operation of the presumption. Legal Aid Queensland stated that:

> despite anti-discrimination legislation in every state and territory as well as Commonwealth legislation, individuals' access to information is restricted or made more difficult by organisations that make arbitrary assessments about whether the individual seeking information has capacity. In our view a statement in the *Privacy Act* that clarifies this issue would significantly assist individuals.[48]

70.34 Others considered that, as a common law presumption already exists, there is no need to include a legislative presumption in the *Privacy Act*.[49] Privacy NSW indicated that, rather than being set out in the *Privacy Act*, a presumption could be incorporated into rules to be developed by the OPC.[50]

70.35 A number of stakeholders indicated that the consideration of the capacity of individuals must be undertaken in a broader context than that arising under the *Privacy*

---

45 Attorney General's Department of New South Wales, *Are the Rights of People Whose Capacity is in Question Being Adequately Promoted and Protected?* (2006), 25.

46 See, eg, Disability Council of New South Wales, *Submission to the Attorney General's Department of New South Wales on Discussion Paper 'Are the Rights of People Whose Capacity is in Question Being Adequately Promoted and Protected?'* June 2006; People with Disability Australia Inc and Blake Dawson Waldron, *Submission to the Attorney General's Department of New South Wales on Discussion Paper 'Are the Rights of People Whose Capacity is in Question Being Adequately Promoted and Protected?'* June 2006; Mental Health Co-ordinating Council, *Submission to the Attorney General's Department of New South Wales on Discussion Paper 'Are the Rights of People Whose Capacity is in Question Being Adequately Promoted and Protected?'* 5 July 2006.

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 61–1.

48 Legal Aid Queensland, *Submission PR 489*, 19 December 2007. See also Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

49 GE Money Australia, *Submission PR 537*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

50 Privacy NSW, *Submission PR 468*, 14 December 2007.

Act.[51] The Department of Human Services warned that capacity issues in a privacy context are related to capacity issues in many administrative decisions that are required to be made when clients interact with service delivery agencies.

> Any policy development in this area in relation to legislative presumptions regarding consent should be able to be replicated in relation to those other administrative decisions. Accordingly, the Department proposes that a whole of Government response be developed in relation to this proposal, which may ultimately proceed in separate legislation to the *Privacy Act*.[52]

70.36 The Law Society of NSW indicated that agencies and organisations collecting sensitive information should not rely on a presumption, but be required to explore the capacity of the individual.[53]

ALRC's view

70.37 The presumption of capacity is an accepted part of the common law in all Australian jurisdictions. The ALRC acknowledges that decisions regarding the handling of personal information are often made in conjunction with many other decisions, all of which may involve considerations of capacity. Given that there are already at least two differing forms of the legislative presumption applying in Australian jurisdictions, the creation of another different (albeit similar) legislative statement, to apply only in the context of the *Privacy Act*, has the potential to create confusion and further add to fragmentation of guardianship and administration laws.

70.38 The presumption of capacity, however, is an important element of the effective operation of the *Privacy Act*. The existence and application of the presumption of capacity should be addressed in guidance to be developed and published by the OPC.[54]

Assessing capacity

70.39 In DP 72, the ALRC proposed that the *Privacy Act* should be amended to provide that if an individual is found to be incapable of making a decision under the *Privacy Act*, an authorised representative may make the decision on behalf of the individual.[55] Proposal 61–1 incorporated a test for determining capacity of the individual, based on similar provisions in the *Health Records Act 2001* (Vic) and the draft *National Health Privacy Code*.[56] The effect of the proposal was to require assessment of capacity in relation to each decision to be made under the *Privacy Act*.

---

51 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007.

52 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

53 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

54 Rec 70–3.

55 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 61–1.

56 *Health Records Act 2001* (Vic) s 85(3); National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4 cl 4(3).

Submissions and consultations

70.40 Many stakeholders supported a specific mechanism in the *Privacy Act* to clarify arrangements for substitute decision making for people with impaired capacity.[57] Some stakeholders acknowledged that capacity is not always easy to assess. It can change and alter over time and may be contextual.

> Capacity is decision specific and impairment of decision-making capacity for some matters (that is, a person has impaired capacity for some types of financial or personal decisions and not others) only is typical. Adults with mental illness will typically have an episodic impairment of their capacity for decision-making. Even during periods when they are unwell, they will typically have capacity for decision-making about some types of matters but not others. Adults with acquired brain injury typically do not identify themselves as having a disability and often present well unless their plausibility is tested, but nevertheless they may have markedly impaired decision-making capacity as a result of gross impulsivity. Again, however, they may be able to make some types of decisions. Adults with dementia typically progress from early dementia, when they may retain or have fluctuating capacity for decision-making for many matters, but progressively become incapable of making decisions about matters.[58]

70.41 A number of stakeholders gave express support for the adoption of a decision-specific assessment of capacity, and the test of capacity proposed in DP 72.[59] Others, however, criticised the requirement that agencies and organisations be required to undertake an assessment of capacity. The Australian Direct Marketing Association (ADMA), for example, indicated that the proposals create a 'layer of complexity and difficulty'; and noted that the assessment of capacity in the context of a direct marketing approach is virtually impossible.[60] Similarly, the Law Council of Australia

---

57 See, eg, Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Guardianship and Administration Committee, *Submission PR 560*, 17 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Optus, *Submission PR 532*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

58 Office of the Public Advocate Queensland, *Submission PR 195*, 12 February 2007.

59 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

60 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

indicated it did not support the proposals, as they do not contemplate the inability to make an assessment in the online environment and other environments in which there is no direct contact with the customer.

70.42 Even some stakeholders that supported the decision-specific assessment approach, acknowledged the difficulty involved in frontline staff of agencies and organisations (perhaps with the exception of health service providers) making an adequate assessment.[61] Carers Australia indicated that assessment of capacity is complex even for trained professionals.[62] The Australian Bankers' Association (ABA) supported the principle that staff should be able to recognise and act upon obvious cases of reduced capacity, but cautioned that bank staff should not be required to make assessments about capacity that would ordinarily be made only by a qualified medical practitioner or psychologist.[63]

70.43 Carers Australia highlighted the need for an appropriate balance between the administrative burden of assessing capacity and the possible consequences of the decision. It suggested that where the impact of the collection, use or disclosure of personal information is minimal, the process to determine capacity could be undertaken relatively quickly and easily, and a more rigorous process used where the potential impact is greater.[64]

70.44 The NSW Guardianship Tribunal had concerns about the proposed provisions, and questioned how an assessment of lack of capacity under the *Privacy Act* would interact with general guardianship laws.

> Does it mean that if a particular agency assesses a person as being incapable of making a particular privacy decision that this decision will then constitute a 'finding' of incapacity? How long will that 'finding' operate? Alternatively, does it mean that the presumption [of incapacity] can only be displaced by a formal finding, such as a determination by a Court or tribunal about the capacity to make a specific privacy decision? Which court or tribunal would make such a finding? The Tribunal has concerns that using the guardianship system to make such findings is unnecessarily legalistic and an inappropriate use of tribunal resources.[65]

70.45 The Tribunal also noted that the ALRC's proposals did not provide a mechanism for resolving disputes over decisions relating to capacity. It suggested that if the OPC is involved in resolving such disputes, it must be supported by a multi-disciplinary panel to deal with the complex issues likely to arise.[66]

---

61 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007.

62 Carers Australia, *Submission PR 423*, 7 December 2007.

63 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

64 Carers Australia, *Submission PR 423*, 7 December 2007.

65 New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007.

66 Ibid.

70.46 Some stakeholders suggested that the proposal should be reworded. The OPC had concerns about the phrase 'or any other circumstance' in defining the reasons why an individual might be found to be incapable of making a decision. The OPC suggested that the term is too broad and might be interpreted in a way that is inconsistent with the ALRC's intention. Further explanatory material on the meaning of the term was supported.[67] The Public Interest Advocacy Centre (PIAC) suggested that the term 'reasonable assistance from another person', which aims to ensure that individuals are given the maximum opportunity to make decisions on their own behalf, might preclude automated or electronic assistance. It suggested the term be replaced with 'despite the provision of all reasonable and appropriate steps being taken to provide assistance'.[68]

70.47 Medicare Australia and Privacy NSW suggested that putting the test of capacity into guidelines would provide greater flexibility in developing practices relevant to the context of the agency or organisation.[69] Privacy NSW noted that:

> The matters for consideration … will differ according to each case and an assessment of capacity to consent should be measured on a sliding scale of factors, some of which relate to age, the ability to communicate consent, the individual's understanding of the issue in question, support from parents or other authorised representatives and the context in which the issues arise.[70]

ALRC's view

70.48 The ALRC received no indication during this Inquiry that the provisions incorporating a test of capacity in the *Health Records Act 2001* (Vic) and *Health Records and Information Privacy Act 2002* (NSW),[71] on which Proposal 61–1 was based, have caused problems in practice. This may be because their operation is limited to health information, and it is more likely in the health services context to have one-on-one assessments by medical professionals who may be better trained and more experienced in making assessments of capacity.

70.49 The ALRC acknowledges that it is difficult to expect frontline staff of agencies and organisations to assess an individual's capacity to make decisions. Assessment of capacity is a complex task, and there is extensive debate in the guardianship and administration community about who is best positioned to make such an assessment, and what guidelines should be followed.[72] Most assessments will rely, at least in part,

---

67 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

68 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

69 Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

70 Privacy NSW, *Submission PR 468*, 14 December 2007.

71 *Health Records Act 2001* (Vic) s 85(3); *Health Records and Information Privacy Act 2002* (NSW) s 7.

72 See, eg, S Ellison and others, *Access to Justice and Legal Needs: The Legal Needs of Older People in NSW* (2004) Law and Justice Foundation of New South Wales; Attorney General's Department of New South Wales, *Are the Rights of People Whose Capacity is in Question Being Adequately Promoted and Protected?* (2006). These issues are not only of concern in Australia: Canadian Centre for Elder Law

on a medical assessment. As the concept of incapacity is a legal concept, however, some argue that neither a medical nor a legal professional alone is equipped to make a true finding of incapacity.[73] The *Older People and the Law* report recommended that SCAG and the Australian Health Ministers' Conference develop and implement a nationally consistent approach to the assessment of capacity.[74]

70.50 The ALRC also agrees that making a 'finding' of incapacity can be problematic for the individual, and could have follow-on legal ramifications for the individual. It is not the ALRC's intention that a finding of incapacity for the purposes of the *Privacy Act* should have an impact on the assessment of the individual's capacity for the purposes of the guardianship and administration regime. This would be inappropriate, particularly where the finding is made by a person not trained to make such a finding.

70.51 While there are real difficulties in the assessment of capacity, the ALRC also notes that, in practice, staff in any agency or organisation must be aware of, and able to recognise, capacity issues when dealing with members of the public. This is not limited to decisions relevant to the *Privacy Act*, but relates to all interactions, including opening bank accounts, entering into contracts, and consenting to medical treatment.

70.52 A test for the assessment of capacity should not be set out in the *Privacy Act*—it is better that these issues be dealt with in guidance developed by the OPC.[75] The guidance should draw on relevant state and territory guardianship and administration legislation that contain definitions of 'capacity', and clarify that these laws apply in the context of the *Privacy Act*. Agencies and organisations should not be expected to make an assessment of capacity of an individual, but must be alert to the possible occurrence of issues concerning capacity, and take such issues into account.

70.53 The ALRC acknowledges that reliance on state and territory legislation that varies from jurisdiction to jurisdiction is not ideal. The task would be made simpler if, as recommended by the House of Representatives Standing Committee on Legal and Constitutional Affairs, uniform legislation was in place with a uniform test for assessing capacity.[76] The inclusion of separate provisions in the *Privacy Act*, however, would ultimately fragment the law on capacity, creating even further confusion and complexity for agencies and organisations.

Studies and British Columbia Law Institute, *A Comparative Analysis of Adult Guardianship Laws in BC, New Zealand and Ontario*, CCELS Report 4; BCLI Report 46 (2006).

73 S Ellison and others, *Access to Justice and Legal Needs: The Legal Needs of Older People in NSW* (2004) Law and Justice Foundation of New South Wales, 328–329; Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), [3.77]–[3.88].

74 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), rec 19.

75 See Rec 70–3 below.

76 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007).

Recognising substitute decision makers authorised by another law

70.54 A third party may be authorised to act as a substitute decision maker by a federal, state or territory law in the following ways:

- appointment by a power of attorney—which lapses if the individual loses capacity;[77]
- appointment under an enduring power of attorney, an instrument of enduring guardianship, or a medical power of attorney—depending on the state or territory, these could cover financial, health or lifestyle decisions;[78]
- appointment as a guardian by a tribunal or board;[79]
- appointment by a tribunal, board or court as an administrator, financial manager or manager;[80] and
- authorisation by a statute to make decisions on behalf of an individual in certain circumstances.[81]

70.55 So long as the extent of the authorisation given by the instrument, appointment or relevant legislation covers matters that are related to the personal information in question, agencies and organisations operating under the *Privacy Act* should recognise these authorisations and allow the person to act as the substitute decision maker for the

---

77 *Powers of Attorney Act 2003* (NSW); *Instruments Act 1958* (Vic); *Powers of Attorney Act 1998* (Qld); *Property Law Act 1969* (WA); *Powers of Attorney and Agency Act 1984* (SA); *Powers of Attorney Act 2000* (Tas); *Powers of Attorney Act 2006* (ACT); *Powers of Attorney Act 1980* (NT).

78 *Powers of Attorney Act 2003* (NSW); *Instruments Act 1958* (Vic); *Powers of Attorney Act 1998* (Qld); *Guardianship and Administration Act 1990* (WA); *Consent to Medical Treatment and Palliative Care Act 1995* (SA); *Powers of Attorney and Agency Act 1984* (SA); *Powers of Attorney Act 2000* (Tas); *Powers of Attorney Act 2006* (ACT); *Powers of Attorney Act 1980* (NT). Western Australia and the Northern Territory have no provision for enduring powers of attorney for medical or lifestyle decisions.

79 *Guardianship Act 1987* (NSW); *Guardianship and Administration Act 1986* (Vic); *Guardianship and Administration Act 2000* (Qld); *Guardianship and Administration Act 1990* (WA); *Guardianship and Administration Act 1993* (SA); *Guardianship and Administration Act 1995* (Tas); *Guardianship and Management of Property Act 1991* (ACT); *Adult Guardianship Act 1988* (NT).

80 *Guardianship Act 1987* (NSW); *Guardianship and Administration Act 1986* (Vic); *Guardianship and Administration Act 2000* (Qld); *Guardianship and Administration Act 1990* (WA); *Aged and Infirm Persons' Property Act 1940* (SA); *Guardianship and Administration Act 1993* (SA); *Guardianship and Administration Act 1995* (Tas); *Guardianship and Management of Property Act 1991* (ACT); *Adult Guardianship Act 1988* (NT).

81 For example, a 'responsible person' under the NSW, South Australian and Tasmanian guardianship legislation is only authorised to give consent to medical or dental treatment—no other decision making is authorised: *Guardianship Act 1987* (NSW) pt 5; *Guardianship and Administration Act 1993* (SA) pt 5; *Guardianship and Administration Act 1995* (Tas) s 39. A statutory health attorney or a principal under an advance health directive under the Queensland legislation has authority to make any decision 'about a health matter' that could have been made by the adult if he or she had capacity: *Powers of Attorney Act 1998* (Qld) ss 36(4), 63.

individual. The substitute decision maker 'stands in the shoes' of the individual, and therefore can provide consent or refuse to provide consent, and have access to information, as if he or she is the individual being represented.[82] Concerns raised in submissions made in response to the Issues Paper *Review of Privacy* (IP 31)[83] indicated that this is not always happening in practice.

70.56 In DP 72, the ALRC proposed a definition of 'authorised representative'.[84] The purpose of the definition was to bring under one definition the multitude of third parties that are authorised by other federal, state or territory laws to make decisions on behalf of an individual who lacks capacity. The proposal was based on the definition of authorised representative in the draft *National Health Privacy Code*,[85] which in turn is based on definitions in the *Health Records and Information Privacy Act 2002* (NSW) and *Health Records Act 2001* (Vic).

Submissions and consultations

70.57 There was support in submissions for including provisions in the *Privacy Act* to ensure that substitute decision makers authorised by another law are recognised for the purposes of the *Privacy Act*.[86] Most concerns raised about the ALRC's proposal related to the wording of the definition.[87]

70.58 As an overall concern, a number of stakeholders highlighted the need to ensure the legislation is not overly complex. The Human Rights and Equal Opportunity Commission noted that the regime must not make it difficult for frontline staff to be able to determine whether someone can act on behalf of another.[88] Similar concerns were raised by GE Money.

> GE considers that it is essential that there is certainty in relation to which individual or individuals may act on behalf of a person who lacks capacity as this protects the vulnerable individual while also allowing the organisation to be sure that it has met its

---

82 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

83 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).

84 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007) Proposal 61–2.

85 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4 cl 1.

86 National Legal Aid, *Submission PR 521*, 21 December 2007; Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

87 See in particular detailed discussion of the wording of the definition in: Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007.

88 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007. See also Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

> legal obligations … In a large organisation with tens of thousands of customers or more it is essential that front line workers have clear rules that are applied to ensure compliance and protection of [an] individual's personal information. Categories of authorised representative must be able to be determined quickly and clearly in any situation.[89]

70.59 Some stakeholders also suggested that there should be a hierarchical list of persons able to be recognised as an authorised representative. This would clarify the procedure to be followed where two or more recognised authorised representatives purported to make decisions on behalf of the individual.[90] It was noted, however, that a standard hierarchy may not be appropriate in all cases. In particular, certain ethnic or Indigenous communities may require a more flexible approach to the recognition of 'authorised representatives'.[91]

ALRC's view

70.60 Substitute decision makers already are empowered by relevant federal, state or territory law to act on behalf of an individual. That law, and where relevant the specific terms of the appointment, will determine whether a third party is able to make decisions on behalf of an individual for the purposes of the *Privacy Act*. It is not necessary for the *Privacy Act* to provide an additional hurdle to the recognition of that substitute decision maker.

70.61 The ALRC acknowledges that some agencies and organisations do not give appropriate recognition to substitute decision makers authorised by law. The problem appears to stem from a lack of understanding of the guardianship and administration and power of attorney laws that apply in each state and territory, a problem that was highlighted by the *Older People and the Law* report.[92] The examples of poor practice, and the complexity of the operation of these laws across state and territory boundaries, influenced the ALRC's attempt, in DP 72, to clarify that legally appointed third parties be recognised specifically for the purposes of the *Privacy Act*.

70.62 Some of the concerns arising from the lack of recognition of substitute decision makers authorised by law can be addressed through appropriate guidance. The ALRC recommends below that the OPC develop and publish guidance to cover these issues.[93] Ultimately, the development of uniform laws for guardianship and administration regimes, including powers of attorney, will be the most effective step in resolving

---

89 GE Money Australia, *Submission PR 537*, 21 December 2007.
90 See, eg, Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.
91 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
92 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007).
93 Rec 70–3.

some of these practical issues. The ALRC endorses the recommendations in the *Older People and the Law* report for uniform laws in this area.[94]

Limits on the liability of agencies and organisations

70.63 If agencies and organisations do not give appropriate recognition to authorised substitute decision makers, the privacy of the individuals being represented may be compromised, and their access to essential services and benefits may be affected. Agencies and organisations, however, must take steps to ensure that only authorised third parties have access to personal information about individuals. As indicated above, this is not an easy task given the myriad of instruments, legislative provisions and appointments that exist.

70.64 In DP 72, the ALRC proposed that the *Privacy Act* should limit the liability of agencies and organisations that rely on a decision of an authorised representative who has exceeded his or her authority, provided that the agency or organisation has taken reasonable steps to validate the authority of the authorised representative.[95]

70.65 A number of key stakeholders supported the proposal.[96] For example, PIAC noted:

> Without this provision, there is a danger that agencies and organisations might adopt an overly-cautious, risk-averse approach when dealing with persons with decision-making disabilities and their authorised representatives. This type of approach could impact adversely on service provision.[97]

70.66 While the ALRC considers that the approach outlined in DP 72 strikes an appropriate balance between facilitating recognition of authorised substitute decision makers and safeguarding against risk of abuse, the ALRC has concluded that the *Privacy Act* is not the right place to insert such a limitation. The issue is not confined to the area of privacy and therefore should be considered as a part of a review of guardianship and administration regimes more generally.

---

94 Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Older People and the Law* (2007), Ch 3.

95 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 61–3.

96 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007.

97 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

Recognising informal representatives

70.67 In DP 72, the ALRC proposed a definition of 'authorised representative' that encompassed only third parties authorised by another law as a substitute decision maker. The ALRC excluded from the definition informal care relationships that are not covered by any legally recognised appointment, whether through some form of power of attorney, or the more formal appointment of a guardian or administrator by a state or territory tribunal, board or court.

Submissions and consultations

70.68 Several stakeholders were concerned that the proposed definition of 'authorised representative' was too narrow, because it did not recognise informal care relationships.[98] This concern was raised by groups and organisations that regularly represent adults with impaired capacity and their carers, and agencies and organisations that provide services to individuals and their carers. These agencies and organisations, particularly in areas related to health information, acknowledged that they rely regularly on decisions made by family and informal carers. For example, Avant Mutual Group noted:

> Consideration needs to be given to adding to the list of authorised representatives some or all of the persons who, acting as the person responsible, can consent to treatment on behalf of the incapacitated person. If for example a spouse, family member or close friend or carer is making decisions for the incapacitated person when it comes to their medical care then so long as any privacy issues relate to the maintenance of the incapacitated person's health and/or is otherwise for their benefit they should be able to consent, request or exercise a right of access, as necessary.[99]

70.69 The Department of Foreign Affairs and Trade (DFAT) noted that it regularly deals with Australians who have become incapacitated while travelling overseas, either through illness or injury. DFAT indicated that, in such circumstances, it takes instructions from next of kin or close family members of those individuals.

> [A] situation may arise where an individual is ill and incapacitated overseas, and there is certain health or other information which is held by the individual's next of kin

---

98 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007; National E-health Transition Authority, *Submission PR 145*, 29 January 2007.

99 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007. See also BUPA Australia Health, *Submission PR 455*, 7 December 2007.

> which, if passed to the relevant authority overseas by an Australian consular officer, would be of benefit to the individual. In this situation, the Department would need to collect the personal information about the individual from the next of kin in order to pass it to the relevant authorities. While UPP 5.1(c) allows for the disclosure of personal information in order to lessen or prevent a serious threat to life, health or safety of the person or the public, there may be situations where no serious threat is apparent, but the disclosure of information would be of benefit to the individual concerned. In such cases, the consent of the next of kin should be enough to allow the disclosure.[100]

70.70 Carers Australia expressed concerns about any individual rights-based approach that fails to recognise that private information about an individual often is intricately associated with others. It noted that the extent to which people choose to share information typically varies in accordance with the closeness and degree of the relationship.

> Caring relationships, by their very definition, involve carers doing things for others (often intimate things) that people are not able to do for themselves due to illness, injury or physical or cognitive disability. While the integrity of each person within the relationship can not be denied, some recognition of the nature of this relationship is warranted. Currently, the privacy legislation fails to recognise the uniqueness of the caring relationship. It can mean that carers do not have access to essential information to act on another person's behalf nor do they receive necessary information to provide the care expected from them. At times, the current privacy laws and their interpretation can make it extremely difficult for a carer to take action to support the person for whom they care. This includes support in relation to financial and health matters, or support for essential changes to living arrangements. In doing so, the Australian Privacy Law fails people with disability, illness or injury and those family and friends who provide care to them.[101]

70.71 A number of stakeholders suggested that the effect of the ALRC's proposed definition of authorised representative would be that—contrary to the intention of state and territory guardianship and administration laws which are based on adoption of the least restrictive option available—organisations and agencies may force carers to obtain a formal care appointment.[102] As noted by Carers Australia, 'it would be absurd to ask the adult child of an ageing parent with dementia to become an administrator when all they merely want to do is to assist their parent with enquiries related to utilities'.[103]

---

100 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.

101 Carers Australia, *Submission PR 423*, 7 December 2007.

102 Australian Guardianship and Administration Committee, *Submission PR 560*, 17 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007; New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007.

103 Carers Australia, *Submission PR 423*, 7 December 2007.

70.72 It was suggested that the *Privacy Act* could incorporate the concept of 'person responsible', as exists in guardianship legislation in a number of jurisdictions, to encourage and support informal care relationships.[104] The New South Wales legislation, which establishes a hierarchy, was given as an example. In the *Guardianship Act 1987* (NSW), a 'person responsible' for another person (other than a child) is defined as:

> (a) the person's guardian, if any, but only if the order or instrument appointing the guardian provides for the guardian to exercise the function of giving consent to the carrying out of medical or dental treatment on the person,
>
> (b) the spouse of the person, if any, if:
>
> (i) the relationship between the person and the spouse is close and continuing, and
>
> (ii) the spouse is not a person under guardianship,
>
> (c) a person who has the care of the person,
>
> (d) a close friend or relative of the person.[105]

70.73 It is important to note, however, that the ability of a 'person responsible' to make decisions on behalf of the individual is at present limited in state and territory legislation to decisions relating to medical and dental treatment that is not classed as special treatment or treatment in the course of a clinical trial.[106] Carers Australia also submitted that these provisions are not systematically recognised or understood.[107]

70.74 The need to make reporting and accountability requirements proportionate to the level of risk was noted by Carers Australia.[108] The NSW Guardianship Tribunal also highlighted the fact that

> it does not follow that because a person is able to access personal information that they will then be able to carry out other actions, for example, a person who is given information about a person's bank accounts does not have authority to operate that account or to access those funds.[109]

70.75 One suggestion was to allow for informal arrangements in situations where individuals need to conduct essential business on a day-to-day basis. Examples given included making small bank withdrawals (up to $100 per fortnight), answering surveys

---

104 Ibid; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

105 *Guardianship Act 1987* (NSW) s 33A. Circumstances in which a person is to be regarded as 'having the care of another person' are set out in s 3D. The meaning of 'close friend or relative' is given in s 3E.

106 See, eg, Ibid, where the concept of 'person responsible' only applies to pt 5 Medical and Dental Treatment.

107 Carers Australia, *Submission PR 423*, 7 December 2007.

108 Ibid.

109 New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007.

on consumer preferences, and buying lottery tickets.[110] It also was suggested that more stringent requirements should apply where serious consequences may flow from disclosure of personal information. For example, more stringent identification requirements should be required for financial matters where there is a greater risk of abuse, and a limit of $5,000 should be placed on the amount of any such transaction.[111]

70.76 On the other hand, some stakeholders were opposed to any expanded recognition of authorised representatives, beyond that recognised by state or territory guardianship and administration legislation. The ABA noted that its members also are bound by the bankers' duty of confidentiality, and that stringent identification checks are necessary. The ABA considered that it would be safer 'for all concerned' if an order or authority for the purposes of the *Privacy Act* were obtained under guardian and administration legislation.[112]

70.77 The NSW Disability Discrimination Legal Centre also opposed allowing informal representatives to act as authorised representatives in relation to non-health related personal information.[113] While acknowledging the problems faced by informal representatives, the Centre considered that the solution is not to dilute the protections of the *Privacy Act*, which might leave a vulnerable person open to abuse. Research estimates that 4.6% of older people experience physical, sexual or financial abuse.[114] It is thought that, in most cases, the perpetrators of abuse are family members or someone who is in a duty of care relationship with the older person. A number of stakeholders noted, however, that risky and abusive practices can be associated with any form of care, whether it be informal, semi-formal or formal.[115]

70.78 The NSW Guardianship Tribunal suggested a number of options that could be introduced to bolster remedies against abuse, if more informal relationships were recognised in the *Privacy Act*, including:

- providing penalties or offences in the Act for the misuse of information gained by an authorised representative;
- giving agencies a discretion not to release information to a responsible person if there are concerns about abuse; and

---

110 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.

111 Office of the Public Advocate Queensland, *Submission PR 195*, 12 February 2007.

112 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

113 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007.

114 Office of the Public Advocate Queensland, *Submission PR 195*, 12 February 2007, citing R Munro, 'Elder Abuse and Legislative Remedies: Practical Remedies' (2002) 81 *Reform* 42.

115 Carers Australia, *Submission PR 423*, 7 December 2007 citing C Tilse, J Wilson and D Setterlund, 'Older People's Assets: A Contested Site' (2005) 24 *Australasian Journal on Ageing* Supplement 51; New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007.

- enabling agencies to make an application to the relevant guardianship tribunal, or make a referral to the relevant public advocate (if available in the state or territory), if concerned about abuse.[116]

70.79 Other stakeholders indicated that existing definitions of 'person responsible' in state and territory guardianship legislation do not go far enough. For example, while existing definitions generally exclude paid carers, hired carers are often authorised to go to a pharmacy to collect medication or otherwise carry out tasks on behalf of the individual they are caring for.[117] Organisations providing housing and care services for persons with a disability—including nursing homes—also regularly act for individuals although they are not legally appointed representatives.[118] Recognition of carers under the age of 18—a common situation where a parent or sibling has a mental health illness—was also an issue of concern.

Options for recognising informal representatives

70.80 Assistance to people with a decision-making disability most commonly occurs through informal processes. As noted above, such assistance is encouraged by Australian guardianship and administration regimes. A Queensland study found that a third of the population has provided asset management assistance to an older person or a person with a disability. Approximately 83% of people providing such assistance did so through informal arrangements, with only 15.4% using an enduring power of attorney and 1.4% using administration orders.[119] Carers Australia suggested that the use of formalised arrangements for the management of personal affairs (as distinct from financial affairs) would be at an even lower level.[120]

70.81 The *Guardianship and Administration Act 2000* (Qld), which implemented the recommendations of the Queensland Law Reform Commission report *Assisted and Substituted Decisions*,[121] recognises that power may be exercised on behalf of an adult with impaired capacity on an informal basis by members of the adult's existing support network.[122] A decision by an informal decision maker may be ratified or approved by the Guardianship and Administration Tribunal.[123] This is the most proactive provision in Australian guardianship and administration legislation for recognition of informal decision making.

---

116 New South Wales Guardianship Tribunal, *Submission PR 403*, 7 December 2007.
117 Confidential, *Consultation PC 175*, Melbourne, 17 October 2007.
118 Confidential, *Submission PR 519*, 21 December 2007.
119 C Tilse, J Wilson and D Setterlund, 'Older People's Assets: A Contested Site' (2005) 24 *Australasian Journal on Ageing* Supplement 51.
120 Carers Australia, *Submission PR 423*, 7 December 2007.
121 Queensland Law Reform Commission, *Assisted and Substituted Decisions*, Report 49 (1996).
122 *Guardianship and Administration Act 2000* (Qld) s 9(2)(a).
123 Ibid s 154.

70.82 A number of Australian jurisdictions have now adopted a mechanism for authorising a 'person responsible' to make decisions on behalf of an individual without the need for a formal appointment.[124] While the definition varies slightly from jurisdiction to jurisdiction, these provisions recognise that family members, close friends and others providing care (other than for remuneration) can make decisions when the individual is unable to do so. As noted above, these provisions apply only in relation to decisions regarding medical and dental treatment.

70.83 Overseas jurisdictions have taken a different approach. In the United Kingdom, a 'best interests' approach has been adopted, which acknowledges that informal carers regularly carry out routine acts and make decisions on behalf of individuals. Section 5 of the *Mental Capacity Act 2005* (UK) provides limited statutory protection from liability for carers and professionals. The protection extends to certain acts performed in connection with the personal care, healthcare or treatment of a person lacking the capacity to consent to those acts. It must be shown that the action was in the best interests of the individual and consistent with the principles set out in the Act.[125] Carers or professionals are not vested with any specific powers or authority to made decisions on behalf of the individual, but are protected from personal liability if their decisions or actions are challenged.

ALRC's view

70.84 Obviously the *Privacy Act* should not allow a third person to have the unfettered ability, without some form of legal authority, to access information about, and make decisions on behalf of, an individual. Even if a limited list of appropriate third persons were set out in the *Privacy Act* (eg, family and carers), this would authorise those third persons to obtain information about, and act on behalf of, the individual without his or her knowledge or consent. While some stakeholders have suggested that this is appropriate for married persons and other family members, such an approach would conflict with the individual-rights focus of the *Privacy Act* and introduce an unacceptable risk of interference with an individual's privacy. The risk would apply not only to vulnerable persons, but to any individual.

70.85 If an informal representative has been authorised (ie, nominated) by the individual to act on his or her behalf, however, this should be acknowledged for the purposes of the *Privacy Act*. This approach, based on the consent of the individual, is

---

124 *Guardianship Act 1987* (NSW) s 33A, with 'person responsible' defined in s 3D; *Guardianship and Administration Act 1986* (Vic) pt 4A, with 'person responsible' defined in s 37; *Powers of Attorney Act 1998* (Qld) s 63 provides for a statutory health attorney, and the role of the statutory health attorney is also recognised in the *Guardianship and Administration Act 2000* (Qld); *Guardianship and Administration Act 1993* (SA) pt 5; *Guardianship and Administration Act 1995* (Tas) s 39, with 'person responsible' defined in s 4. The issue is under consideration in the ACT: ACT Government Department of Justice and Community Safety, *Consenting to Treatment: Discussion Paper* (2007).

125 This provision was based on the recommendations contained in Law Commission of England and Wales, *Mental Incapacity*, Report 231 (1995). The Law Reform Commission of Ireland has recently recommended adopting the same approach: Law Reform Commission of Ireland, *Vulnerable Adults and the Law*, LRC 83 (2006).

consistent with the individual rights focus of the *Privacy Act* and provides a remedy for individuals and their informal representatives where incapacity is anticipated and the nomination is made prior to the loss of capacity.

70.86 The ALRC's recommendations in relation to nominees are discussed in detail below.

Third party representatives acting with consent

Nominees

70.87 In DP 72, the ALRC asked two questions about nominees: whether the *Privacy Act* should be amended expressly to allow a third party nominated by an individual to make a decision under the *Privacy Act*, either for one-off or long term arrangements; and whether nominees should be recognised as 'authorised representatives'.[126]

Submissions and consultations

70.88 Most stakeholders that addressed the matter supported the recognition of nominees in the *Privacy Act*.[127] The Office of the Victorian Privacy Commissioner noted that this approach is consistent with privacy laws by 'allowing an individual the maximum amount of autonomy in decisions concerning their own personal information, to the extent that is reasonable and practicable'.[128] The nominee arrangement also was seen as giving recognition to the fact that capacity is not a fixed concept and can change over time.[129]

70.89 Some of the support for a nominee arrangement was qualified. Stakeholders highlighted particular concerns about how such an arrangement would operate in practice, including:

---

126 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Questions 61–2, 62–1.

127 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007; P Youngman, *Submission PR 394*, 7 December 2007; Festival of Light Australia, *Submission PR 354*, 1 December 2007.

128 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

129 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

- the need for clear guidance on when the arrangement can be used;[130]
- the need for safeguards to be put in place to ensure that the individual has capacity at the time the nomination is made;[131]
- the requirement of a close and continuing relationship between the individual and the nominated person—ie, the nominee should fall within a definition of 'person responsible';[132]
- the need for a process to ensure that the nomination is up-to-date and reviewed at times when the individual has capacity;[133]
- subjecting the nomination process, particularly in health care contexts, to guidelines and rules that would promote the inclusion of time limits concerning the duration of the nomination;[134]
- the development of appropriate safeguards for agencies and organisations that rely on decisions by, and directions of, nominees—including an entitlement to assume that the appointment is valid and enduring unless otherwise notified;[135]
- the need to ensure that individuals are informed of any changes made by the nominee;[136]
- the identification of avenues for review of, or challenge to, a nomination;[137] and
- a recognition of existing protections provided for in state and territory guardianship legislation that should apply in the event of the abuse of the position by the nominee.[138]

70.90 Carers Australia noted that the nominee arrangement should not create practical difficulties for carers who must organise arrangements across all relevant agencies and organisations.

---

130 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

131 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.

132 Avant Mutual Group Ltd, *Submission PR 421,* 7 December 2007. The term 'person responsible' features in guardianship and administration legislation in a number of jurisdictions: see, eg, *Guardianship Act 1987* (NSW) s 33A with 'person responsible' defined in s 3D.

133 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

134 Medicare Australia, *Submission PR 534,* 21 December 2007.

135 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; Law Council of Australia, *Submission PR 527,* 21 December 2007.

136 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

137 Australian Guardianship and Administration Committee, *Submission PR 560,* 17 January 2008.

138 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495,* 19 December 2007.

> A likely scenario might involve negotiating such 'semi-formal' arrangements with Centrelink, phone company, gas company, electricity company, housing department/real estate agent, various disability or aged care providers, private health fund etc. Making these arrangements should not add another layer of administrative burden for carers. For carers who may be struggling to deal emotionally and practically with the impairment or disability of a loved one, this is yet another responsibility they are expected to undertake with little assistance or guidance. For this reason, simplicity and consistency in the establishment of such arrangements would be essential.[139]

70.91 While Medicare Australia supported the existence and operation of a nominee arrangement, it did not consider it necessary to give it a legislative basis in the *Privacy Act*.[140] Carers Australia did not support a legislative provision that duplicates the existing process of appointing an enduring power of attorney.[141] Similar concerns were expressed by the business sector.

> It is open to people to make a formal nomination by way of an enduring power of attorney. Informal nominations should be approached with extreme caution and on their own should not be sufficient. There must be a close and continuing relationship between the incapacitated person and the nominated person, so that even without the nomination the nominated person could be considered a responsible person.[142]

70.92 A number of stakeholders queried whether a nomination should be made in writing. They suggested that verbal nominations and revocation of nominations also should be recognised.[143]

70.93 In contrast, GE Money noted:

> There are very real issues for organisations in determining whether it is appropriate to disclose information to anyone other than the individual concerned. There are significant issues involved in correctly identifying a third party, even if the organisation is clear that a third party is authorised by the individual to receive information. While the NPPs may currently support verbal consent it should be recognised that an organisation faces very real issues in this regard. If there is no record of the individual having provided their consent to a disclosure to a third party the organisation is unable to establish the basis on which they have acted if the decision to disclose information is later challenged.[144]

---

139 Carers Australia, *Submission PR 423*, 7 December 2007.

140 Medicare Australia, *Submission PR 534*, 21 December 2007.

141 Carers Australia, *Submission PR 423*, 7 December 2007.

142 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

143 Medicare Australia, *Submission PR 534*, 21 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; National Relay Service, *Submission PR 484*, 18 December 2007.

144 GE Money Australia, *Submission PR 537*, 21 December 2007. See also Law Council of Australia, *Submission PR 527*, 21 December 2007 which supported that nomination of third parties be subject to a written requirement.

70.94 Other stakeholders pointed out, however, that there are a number of options for verbal consent available to consumers and service providers. These include the practice of accepting a verbal consent provided that written consent is to be given later, and recording a verbal consent, allowing for a quicker resolution to the problem while still ensuring that the consent is properly recorded for record-keeping purposes.[145]

70.95 The OPC acknowledged that the nomination and verification requirements to be applied will vary, according to the circumstances.

> Some circumstances require a more rigorous process for nomination and verification than others due to the potential consequences of the disclosure of personal information. In general, the [OPC] considers that it is good practice to obtain consent in writing. There may be circumstances, however, where it is appropriate for an agency or organisation to accept verbal consent provided that robust identification and security procedures have been followed.[146]

ALRC's view

70.96 Nominee arrangements provide flexibility for individuals to decide who can act as their 'agent' for the purposes of the *Privacy Act*, and also operate as a useful mechanism in situations where an individual has limited, intermittent or declining capacity.

70.97 The ALRC notes that a number of agencies and organisations already use nominee arrangements for the benefit of their customers. For example, the Centrelink nominee arrangements, despite being subject to some criticism, are generally well received and widely utilised. The Office of the Public Advocate Queensland indicated that, without this arrangement, many people with an impaired capacity would not have received benefits to which they were entitled.[147]

70.98 The ALRC acknowledges that there are arguments against including a nominee arrangement in the *Privacy Act*. On balance, however, the ALRC sees advantages in setting out nominee arrangements in the *Privacy Act*. The rationale may be summarised as follows:

- The nomination should have an enduring quality—that is, the nomination should continue to be valid if the individual loses capacity. The ALRC is concerned that without any legislative provision to the contrary, the consent of the individual to the nomination may be considered to have been withdrawn at the time the individual loses capacity.

---

145 Australian Collectors Association, *Submission PR 505*, 20 December 2007. This submission was supported by Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007.

146 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

147 Office of the Public Advocate Queensland, *Submission PR 195*, 12 February 2007.

- The relationship should be given a legislative basis with some minimum requirements about how it will operate in practice. The third party nominee has ongoing powers to make decisions on behalf of an individual, and this situation could be subject to abuse.

- Although the ALRC is not recommending that nominee arrangements be a mandatory requirement, a legislative basis for the nominee arrangement will help to raise the profile of the existence of such arrangements.

70.99 The *Privacy Act* provisions establishing nominee arrangements should not be overly prescriptive. They must retain flexibility for agencies and organisations to develop practices and procedures that are consistent with their broader operations. Agencies and organisations also may be subject to other obligations, such as the bankers' duty of confidentiality or particular legislative provisions, which place limits on third party decision making. Each agency and organisation must consider the extent to which it is able to recognise and act upon decisions made by a nominee.

70.100 Some circumstances require a more rigorous process for nomination and verification than others, due to the potential consequences of the disclosure of personal information or the transaction involved. For example, a financial institution may establish a nominee arrangement that has effect for the purposes of the *Privacy Act*, but does not extend to a nominee withdrawing funds from an account on behalf of the individual. On the other hand, a body such as Optus, which already has a nominee arrangement in place, can harmonise nominee arrangements for the purposes of the *Privacy Act* with arrangements that allow the nominee to make changes to the contracted service on behalf of the individual.

70.101 The ALRC recommends that the following elements of a nominee arrangement be set out in the *Privacy Act*:

- A nomination should be able to be made by the individual, or by a third party authorised by another federal, state or territory law as the substitute decision maker for the individual. The substitute decision maker may nominate himself or herself or an alternative third party as the nominee. While it is not necessary that an authorised substitute decision maker be registered as a nominee for the agency or organisation to recognise that person, the nominee arrangement is a convenient way for the substitute decision maker to be recognised for ongoing dealings with the agency or organisation. A similar approach is taken under the Centrelink nominee arrangements.

- The nominee may be any individual or an entity. The person making the nomination should not be limited to a list of suitable persons by category. Provision for nominating an entity would overcome concerns raised in this Inquiry about recognising the staff of care and accommodation services,

including nursing homes, who regularly act on behalf of, or assist, individuals with routine daily tasks. If an entity were nominated, an authorised staff member of that entity would be able to act as the individual's nominee, overcoming problems regarding staff turnover that are associated with nominating individuals.

- The nominee should have an obligation to act in the best interests of the individual on whose behalf the nominee acts. This would establish a basic level of responsibility for the nominee, and a basis upon which an individual could seek redress through the courts in cases where serious harm has been done to the individual by the nominee. It is common for persons appointed as a substitute decision maker to be subject to some kind of obligation, such as the requirement to act honestly and with reasonable diligence,[148] to protect the interests of the donor of the power,[149] or to act in the best interests of the represented person.[150] Under the Centrelink arrangements, a nominee has a duty to 'act in the best interests of the principal' at all times.[151]

- The nomination should be able to be revoked by the individual, an authorised substitute decision maker, the nominee or the agency or organisation.

70.102 There are a number of other matters that should be considered by an agency or organisation in developing a nominee arrangement. While these elements do not need to be specified in legislation, it may be appropriate for the OPC to provide guidance on these issues as part of its guidance on developing and administering nominee arrangements.[152] Such issues may include:

- provision for verbal, or the requirement of written, authorisation of nominees, and revocation of nominations;

- time limitations, if any, to be placed on nominations;

- dealing with conflicting instructions from an individual and his or her nominee;

- whether to allow for multiple nominees, and how to deal with a conflict of instructions from multiple nominees;

- circumstances in which an agency or organisation should revoke a nomination;

---

148 *Guardianship and Administration Act 2000* (Qld) s 35; *Powers of Attorney Act 1998* (Qld) s 66; *Powers of Attorney and Agency Act 1984* (SA) s 7.

149 *Powers of Attorney Act 2000* (Tas) s 32.

150 *Guardianship and Administration Act 1986* (Vic) s 28; *Guardianship and Administration Act 1995* (Tas) s 27.

151 *Social Security (Administration) Act 1999* (Cth) s 123O.

152 Rec 70–3.

- notifying all parties involved when a nomination is revoked; and
- cost effective procedures that can be built into the nominee arrangement to reduce the risk of abuse, and identify and deal with situations of abuse.

Recommendation 70–1 The *Privacy Act* should be amended to include the concept of a 'nominee' and provide that an agency or organisation may establish nominee arrangements. The agency or organisation should then deal with an individual's nominee as if the nominee were the individual.

Recommendation 70–2 The *Privacy Act* should be amended to provide for nominee arrangements, which should include, at a minimum, the following elements:

(a) a nomination can be made by an individual or a substitute decision maker authorised by a federal, state or territory law;

(b) the nominee can be an individual or an entity;

(c) the nominee has a duty to act at all times in the best interests of the individual; and

(d) the nomination can be revoked by the individual, the nominee or the agency or organisation.

Other third parties providing assistance

70.103 While nominee arrangements are suitable for establishing long-term recognition of nominated substitute decision makers, there are many other situations where an individual may wish a third party to be involved in assisting with decision making under the *Privacy Act*. The third parties involved may be carers, spouses, parents, adult children, interpreters, counsellors, legal representatives or any other person chosen by the individual.

70.104 As outlined above, there is nothing in the *Privacy Act* that prevents a third party from providing assistance to the individual where this is done with the consent of the individual. Where the assistance requires the third party to have access to the personal information of the individual, the individual can provide consent for the agency or organisation to disclose the information to the third party. Concerns were expressed, however, that such consensual arrangements are not implemented consistently or recognised by agencies and organisations.

70.105 In DP 72, the ALRC proposed that the OPC develop and publish guidance on practices and procedures allowing for the involvement of third parties to assist an individual to make and communicate privacy decisions.[153] Guidance provides agencies and organisations with the confidence to introduce appropriate arrangements that are consistent with the *Privacy Act*. A number of stakeholders supported the proposal.[154]

70.106 A particular issue was raised by the National Relay Service (NRS). The NRS uses trained officers to relay calls between people who are deaf, hearing-impaired or speech-impaired, and members of the wider community. The NRS acts as a central link in the call by relaying what is said by both parties. Services are provided via phone, computer, mobile phone or teletypewriter (TTY). The NRS indicated that there often are problems with the recognition and authorisation of NRS officers facilitating communication between an individual and service providers, particularly financial institutions dealing with credit matters.[155] It suggested a number of ways the *Privacy Act* could be amended to ensure that NRS operators can provide the necessary services without express or written authorisation from the individual, including a specific exception for use and disclosure of information to the NRS for the purposes of carrying out its functions.[156]

70.107 While there is no need to amend the *Privacy Act* to deal specifically with the problems raised by the NRS, OPC guidance on third party representatives should make reference to NRS services and the consensual basis on which they operate.

Married persons

70.108 The Festival of Light Australia suggested that the *Privacy Act* be amended to provide a presumption that a spouse may give consent, make a request or exercise a right of access on behalf of the other spouse. The Festival of Light indicated the need for the amendment because 'married couples have, by the act of marrying one another, entered into a unique social and legal relationship'. It suggested that the presumption

---

153 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 62–1.

154 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Festival of Light Australia, *Submission PR 354*, 1 December 2007.

155 Written authorisation from the individual is required before third parties may exercise rights of access to credit reporting information relating to the individual: *Privacy Act 1988* (Cth) s 18H(3). This is sometimes interpreted to apply to any disclosure to a third party. This requirement is discussed in Ch 59.

156 National Relay Service, *Submission PR 484*, 18 December 2007. Although note that Optus considers that the disclosure is sufficiently authorised by the *Telecommunications Act 1997* (Cth), and that there is no need to amend the *Privacy Act 1988* (Cth): Optus, *Submission PR 532*, 21 December 2007.

should operate in the absence of a specific instruction from a married person to the contrary.[157] This suggestion was echoed in a number of comments and submissions received from individuals during this Inquiry.[158]

70.109 Applying a presumption that a spouse is acting with the consent of his or her partner is contrary to the individual rights approach of the *Privacy Act* and would introduce an unacceptable risk of interference with an individual's privacy. The ALRC acknowledges the frustrations encountered by many married persons trying to operate within the boundaries of the *Privacy Act*, such as when trying to sort out a utility or credit card bill formally in the other partner's name. The ALRC's recommendations in relation to recognising nominee arrangements in the *Privacy Act*, together with clear guidance on how such arrangements can operate, should help to facilitate easier interactions between agencies and organisations and their married or partnered customers and clients.

Implementing third party arrangements

70.110 In DP 72, the ALRC put forward a number of proposals aimed at assisting the implementation of provisions and processes relating to third party representatives, which would require:

- the OPC to develop and publish guidance relating to assessing the capacity of an individual;[159] and practices and procedures for allowing the involvement of third parties to assist an individual to make and communicate privacy decisions;[160] and

- agencies and organisations that handle personal information about individuals incapable of making a decision to address in their Privacy Policies how such information is managed;[161] and ensure that their staff are trained adequately to assess the decision-making capacity of individuals.[162]

157 Festival of Light Australia, *Submission PR 354*, 1 December 2007.

158 See, eg, R Minahan, *Submission PR 482*, 13 December 2007; B Such, *Submission PR 71*, 2 January 2007; *ALRC National Privacy Phone-in*, June 2006, Comments #1203, #778, #195. But there was also support for individual privacy within a marriage: *ALRC National Privacy Phone-in*, June 2006, Comment #840.

159 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 61–4.

160 Ibid, Proposal 62–1.

161 Ibid, Proposal 61–5.

162 Ibid, Proposal 61–6.

Submissions and consultations

70.111 Stakeholders generally agreed that the OPC should provide guidance in these circumstances,[163] and in so doing should consult with banks,[164] people with disabilities, their carers and disability services,[165] peak disability advocacy groups, disability discrimination commissioners and others with expertise and experience on capacity issues.[166]

70.112 In relation to the guidance on assessing capacity, GE Money opposed the proposal, on the basis that decisions regarding capacity have an impact beyond privacy, and the OPC is not the appropriate body to be providing guidance on how to assess capacity.[167] In relation to the guidance on involving third parties assisting to make and communicate privacy decisions, the ADMA expressed doubts about the effectiveness of the proposal.[168]

70.113 A number of submissions supported the proposal that agencies and organisations that handle personal information about adults incapable of making a decision should include information about the management of such information in their Privacy Policy.[169] Optus supported an alternative proposal, that such information be required to be provided on request, rather than required to be included in Privacy

---

163 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Australian Mercantile Agents Association, *Submission PR 508*, 21 December 2007; Australian Investigators Association, *Submission PR 507*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Festival of Light Australia, *Submission PR 354*, 1 December 2007.

164 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

165 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.

166 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

167 GE Money Australia, *Submission PR 537*, 21 December 2007.

168 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

169 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007.

Policies.[170] The OPC recognised the possible compliance burden on business, given that almost all agencies and organisations will deal at some time with capacity issues. The OPC suggested rewording the proposal so that agencies and organisations, 'where practicable', should include the information in their Privacy Policies.[171]

70.114 There were some concerns about the ALRC's proposal that agencies and organisations that regularly handle personal information about adults incapable of making a decision ensure that staff are trained adequately to assess the decision-making capacity of individuals.[172] While there was support for the proposal,[173] the Australian Taxation Office (ATO) considered it excessive, suggesting instead that the training requirement be

> confined to those bodies whose functions specifically include service provision to client groups with these special needs (such as the Department of Health and Ageing) … For other agencies such as the Tax Office, providing meaningful training on these issues for all staff would not be an efficient or effective use of resources.[174]

70.115 The ATO acknowledged, however, that it regularly deals with individuals with capacity issues and that its staff must be conscious of relevant issues when dealing with these individuals or their carers. The ABA suggested that basic training in behavioural warning signs would be appropriate, but stressed that bank staff should not be required to make assessments about capacity that would ordinarily only be made by a qualified medical practitioner or psychologist.[175]

ALRC's view

OPC guidance

70.116 Guidance, to be developed and published by the OPC, is essential to facilitate the effective use of third party representatives consistent with the *Privacy Act*. Areas that should be included in the guidance include:

- **The involvement of third parties, with the consent of an individual, to assist the individual to make and communicate privacy decisions.** The consensual

---

170 Optus, *Submission PR 532*, 21 December 2007.

171 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

172 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 61–6.

173 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Office of the Public Advocate Queensland, *Submission PR 435*, 10 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007.

174 Australian Taxation Office, *Submission PR 515*, 21 December 2007. The ATO has over 21,000 employees.

175 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

involvement of third parties is consistent with the *Privacy Act*, but there appears to be some confusion in practice about when third parties—including interpreters, counsellors and legal representatives—can assist the individual to access personal information about himself or herself and communicate with an agency or organisation in relation to issues under the *Privacy Act*.

- **Establishing and administering nominee arrangements.** The new provisions of the *Privacy Act* will need to be explained and agencies and organisations encouraged to establish nominee arrangements. Many aspects of a nominee arrangement will be left for each agency or organisation to develop to suit its own purposes, but OPC guidance on these issues will assist agencies and organisations to consider what is appropriate in their circumstances.

- **Identifying and dealing with issues concerning capacity, including the application of a presumption of capacity.** The need to consider such issues is relevant not only in the privacy context, but in all dealings between the agency or organisation and an individual who may have capacity issues. While the OPC could draw on publications already in the public domain regarding capacity and recognition of substitute decision makers,[176] it would be necessary to put these practices into the context of decision making under the *Privacy Act*.

- **Recognising and verifying the authority of substitute decision makers authorised by a federal, state or territory law.** The existence of inconsistent state and territory laws makes this a difficult area for agencies and organisations to navigate. As with capacity issues, the need to recognise and verify the authority of substitute decision makers is not limited to the privacy context. Where properly authorised substitute decision makers are not recognised for the purposes of the *Privacy Act*, however, this can have an impact on access to services and benefits for individuals with an incapacity.

70.117 As suggested in submissions, it will be important for the OPC to consult with people with disabilities, their carers and disability services, peak disability advocacy groups, and disability discrimination commissioners and others that have worked on capacity issues. The best practice guide developed by Privacy NSW on *Privacy and People with Decision-Making Disabilities*, which includes a checklist for dealing with capacity and alternative decision-making issues, is a good example of guidance that highlights issues concerning capacity and dealing with authorised substitute decision makers.

---

176 Examples of capacity checklists and guides include: P Darzins, W Molloy and D Strang (eds), *Who Can Decide?: The Six Step Capacity Assessment Process* (2005); Disability Advocacy NSW, *Capacity Checklist* <www.da.org.au/publications.asp> at 5 May 2008.

Information in Privacy Policies

70.118 While there was support in submissions to require agencies and organisations to address in their Privacy Policies how information relating to individuals with an incapacity will be handled, the ALRC does not recommend making this a requirement in all Privacy Policies.[177] The personal information of individuals lacking decision-making capacity will not be handled differently from the personal information of other individuals—the only difference will be that communication with the agency or organisation may be through a third party instead of directly with the individual.

70.119 Agencies and organisations should advise their clients and customers about the third party arrangements that operate in that agency or organisation. This extends to third party arrangements for all individuals, not only those with an incapacity, and includes nominee arrangements if such arrangements have been established.

70.120 The best way for agencies and organisations to communicate their practices for dealing with third parties is to develop formats that can be targeted to the clients and customers of, and the particular processes adopted by, the agency or organisation. The guidance to be developed by the OPC on third party representatives should highlight the benefits of making this information publicly available.

Training requirements

70.121 The ALRC recommends that agencies and organisations that regularly handle personal information about individuals with a temporary or permanent incapacity should ensure that relevant staff interacting with those individuals are trained adequately to recognise capacity issues, and know how to deal with them. This is not the same as expecting staff to make an assessment of capacity, a decision that should be undertaken by professionals consistent with laws and guidelines established by guardianship and administration legislation in each state and territory. Staff dealing with the general public should, however, be aware of problems that may arise in dealing with clients who have capacity issues. Training also should deal with recognition of third parties authorised as substitute decision makers under another federal, state or territory law.

---

177 The ALRC recommends that agencies and organisations should set out clearly expressed policies on their handling of personal information in a Privacy Policy, including how they collect, hold, use and disclose personal information: see Rec 24–1.

Recommendation 70–3 The Office of the Privacy Commissioner should develop and publish guidance for dealing with third party representatives, including in relation to:

(a) the involvement of third parties, with the consent of an individual, to assist the individual to make and communicate privacy decisions;

(b) establishing and administering nominee arrangements;

(c) identifying and dealing with issues concerning capacity; and

(d) recognising and verifying the authority of substitute decision makers authorised by a federal, state or territory law.

Recommendation 70–4 Agencies and organisations that regularly handle personal information about adults with limited or no capacity to provide consent, make a request or exercise a right under the *Privacy Act*, should ensure that relevant staff are trained adequately in relation to issues concerning capacity, and in recognising and verifying the authority of third party representatives.

Part J

Telecommunications

71. *Telecommunications Act*

Contents

Introduction

71.1 Telecommunications service providers handle personal information about their customers in order to supply them with services such as landline telephone services, mobile telephone services and internet services. Before the introduction of the private sector provisions of the *Privacy Act 1988* (Cth), the use and disclosure of information collected and held by telecommunications service providers was regulated by industry-specific legislation[1] and instruments.[2] Since the introduction of the private sector provisions, however, the handling of personal information by telecommunications

1 *Telecommunications Act 1991* (Cth) s 88; *Telecommunications Act 1997* (Cth) pt 13.

2 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) (deregistered on 29 Oct 2001); *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

service providers is governed by both the *Telecommunications Act 1997* (Cth) and the *Privacy Act*, as well as other industry-specific instruments, such as licences and codes.

71.2 A number of recent inquiries have considered the interaction between telecommunications industry-specific regulation and the *Privacy Act.* In 2005, the Office of the Privacy Commissioner (OPC) considered this interaction as part of its review of the private sector provisions of the *Privacy Act* (OPC Review).[3] The OPC's recommendations on this issue are discussed throughout this chapter.

71.3 In 2005, the Senate Legal and Constitutional References Committee recommended that the ALRC conduct a comprehensive review of privacy that considered, among other things, the interaction between the *Privacy Act* and the *Telecommunications Act*.[4] In addition, in 2006, a review of the regulation of business in Australia concluded that the need to clarify and harmonise the relationship between the *Privacy Act* and the *Telecommunications Act* should be considered as part of a wider review of privacy laws.[5]

71.4 On 8 May 2006, the ALRC received a letter from the then Attorney-General, the Hon Philip Ruddock MP, stating that it would be desirable for the ALRC to consider the interaction between the *Privacy Act* and the *Telecommunications Act* during the course of this Inquiry.

71.5 This chapter first considers the provisions of the *Telecommunications Act* and how they interact with the *Privacy Act.* The next section examines whether telecommunications-specific privacy legislation is still required. The chapter then looks at whether the *Telecommunications Act* provides adequate protection of personal information. This latter section of the chapter considers the regulatory gap caused by the small business exemption; the impact of new privacy-invasive technologies; and whether a contravention of Part 13 of the *Telecommunications Act* should attract a civil or criminal penalty. The final section of the chapter considers the role of the OPC and the Australian Communications and Media Authority (ACMA) under the *Telecommunications Act.*

71.6 Chapter 72 also considers whether the *Telecommunications Act* provides adequate protection of personal information, and focuses on the exceptions to the use and disclosure offences and the protection of personal information held on public number directories.

---

3 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005).

4 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), recs 1, 9.

5 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), rec 4.48.

71.7 Chapter 73 considers the *Telecommunications (Interception and Access) Act 1979* (Cth), the *Spam Act 2003* (Cth), and the *Do Not Call Register Act 2006* (Cth), as well as the functions of the various bodies with responsibility for privacy in the telecommunications industry. The privacy of internet users and users of wireless technologies is discussed more generally in Chapter 11.

Telecommunications Act 1997 (Cth)

71.8 The *Telecommunications Act* regulates the activities of a number of participants in the telecommunications industry, including 'carriers' and 'carriage service providers'. The statutory definitions of these terms are complex. Essentially, a 'carrier' is the holder of a 'carrier licence'[6]—a type of licence required before certain infrastructure can be used to carry communications by means of guided and unguided electromagnetic energy.[7] A 'carriage service provider' is a person who makes use of the infrastructure owned by a carrier to carry these types of communications.[8]

71.9 Part 13 of the *Telecommunications Act* regulates the use and disclosure of information obtained by certain bodies during the supply of telecommunication services. It makes it an offence (punishable by up to two years imprisonment) for certain participants in the telecommunications industry (referred to in this chapter as 'telecommunications service providers')—namely, carriers, carriage service providers, telecommunications contractors and their employees; eligible number-database operators;[9] and emergency call persons—to use or disclose information or a document relating to the:

- contents or substance of a communication carried, or being carried, by a carrier or carriage service provider;
- carriage services supplied or intended to be supplied by a carrier or carriage service provider; or
- affairs or personal particulars (including any unlisted telephone number or any address) of another person.[10]

71.10 The Act specifies a number of exceptions to these 'primary use/disclosure offences'.[11] The Act also regulates the secondary use and disclosure of protected

---

6 *Telecommunications Act 1997* (Cth) s 7. A carrier licence is granted under s 56 of the Act.
7 Ibid ss 7, 42.
8 Ibid ss 7, 16, 87.
9 Ibid s 272. There are currently no eligible number-database operators as no determination is in force under s 472(1).
10 Ibid ss 276–278. Part 13 protects information or a document about a communication, but does not protect the content or substance of the communication. The content or substance of a communication is protected under the *Telecommunications (Interception and Access) Act 1979* (Cth).
11 Ibid ss 279–294. These exceptions are discussed in detail in Ch 72.

information.[12] For example, a person to whom information was disclosed because the disclosure was required or authorised by or under law is prohibited from using or disclosing the information, unless the further use and disclosure is also required or authorised by or under law.[13] A person who contravenes the secondary use and disclosure provisions is guilty of an offence punishable by up to two years imprisonment.[14]

71.11 Part 6 of the *Telecommunications Act* deals with the development of industry codes and standards for particular industry activities. Industry codes and standards developed under the Act can deal with privacy, including the protection of personal information.[15] An industry code or standard cannot, however, derogate from the requirement of the *Privacy Act* or a privacy code approved under the *Privacy Act*.[16]

71.12 The *Privacy Act* regulates many aspects of the handling of personal information by telecommunications service providers. For example, a telecommunications service provider that is not a small business must collect information in compliance with National Privacy Principle (NPP) 1, and must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date as required under NPP 3. Therefore, both Part 13 of the *Telecommunications Act* and the NPPs regulate the handling of personal information. The interaction between these provisions is discussed further below.

71.13 In 1999, the Australian Communications Industry Forum (ACIF) (now Communications Alliance), a body that represents the interests of the communications industry, developed and registered the *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* (the Code) under Part 6 of the *Telecommunications Act*.[17] The Code expanded on the privacy protections of Part 13 and addressed matters that are not dealt with in the Part, such as how information should be collected, stored and handled. These requirements were based on the National Principles for the Fair Handling of Personal Information,[18] which later became the NPPs under the *Privacy Act*. The Code was considered to be unnecessary when the private sector provisions of the *Privacy Act* came into force, and was deregistered in 2001.

---

12 Ibid ss 296–303A.
13 Ibid s 297.
14 Ibid s 303.
15 Ibid s 113(3)(f).
16 Ibid s 116A.
17 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999).
18 Office of the Privacy Commissioner, *National Principles for the Fair Handling of Personal Information* (1999).

Interaction between the *Privacy Act* and the *Telecommunications Act*

The type of information protected

71.14 The *Privacy Act* protects 'personal information' which is currently defined as:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[19]

71.15 In Chapter 6, the ALRC recommends that the *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.[20] Generally, the privacy principles in the *Privacy Act* only apply to personal information that is held, or collected for inclusion, in a 'record'.[21]

71.16 As noted above, Part 13 of the *Telecommunications Act* regulates the use or disclosure of information or a document relating to the:

- contents or substance of a communication carried, or being carried, by a carrier or carriage service provider;
- carriage services supplied or intended to be supplied by a carrier or carriage service provider; or
- affairs or personal particulars (including any unlisted telephone number or any address) of another person.[22]

71.17 Information or a document protected under Part 13 could relate to many forms of communications, including fixed and mobile telephone services, internet browsing, email and voice over internet telephone services. For telephone-based communications, this would include subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet-based applications, the information protected under Part 13 would include the Internet Protocol (IP) address used for the session, and the start and finish time of each session.

---

19 *Privacy Act 1988* (Cth) s 6(1).

20 Rec 6–1.

21 The IPPs expressly refer to collection of personal information by agencies for inclusion in a 'record', storage and security of 'records', access to 'records' and so on. Section 16B provides that the Act applies to the collection of personal information by an organisation only if the information is collected for inclusion in a record or is held by the organisation in a record. The privacy principles also apply to the collection of information for inclusion in a 'generally available publication'. The definition of 'generally available publication' is discussed in Ch 6.

22 *Telecommunications Act 1997* (Cth) ss 276–278.

71.18 Information or a document will be protected by Part 13 only if it comes to a person's knowledge, or into the person's possession in certain circumstances. For example, s 276 provides that information or documents protected under that section will be protected if they come to a person's knowledge, or into the person's possession:

- if the person is a current or former carrier, carriages service provider or telecommunications contractor, in connection with the person's business as such a carrier, provider or contractor; or

- if the person is an employee of a carrier, carriage service provider, telecommunications contractor, because the person is employed by the carrier or provider in connection with its business as such a carrier, provider or contractor.

71.19 A telecommunications service provider may collect information that does not come into a person's knowledge or possession in the circumstances specified in Part 13. For example, a carriage service provider may buy a customer list for direct marketing purposes; or collect information when offering services that are not related to its business as a carriage service provider, for example, an online music business. This information will not be regulated by Part 13. If it is personal information, however, it may be regulated under the *Privacy Act*.

71.20 The Australian Privacy Foundation submitted that the reference to 'the affairs or personal particulars … of another person' in the *Telecommunications Act* is too narrow and that 'personal information', as defined in the *Privacy Act*, is a more appropriate term for use in the *Telecommunications Act*.[23]

71.21 In the ALRC's view, however, the *Telecommunications Act* protects a broader range of information than 'personal information' in the context of information or documents that are obtained in the circumstances outlined in Part 13. Information or a document protected under Part 13 (including information or a document relating to the contents or substance of a communication carried, or being carried) would include 'personal information' if the information or document was:

- about an individual whose identity was apparent, or could reasonably be ascertained, from the information or document; and

- held, or collected for inclusion in a record.

71.22 As noted in Chapter 6, while stand-alone telephone numbers, street addresses and IP addresses may not be 'personal information' for the purposes of the *Privacy Act*, such information may become personal information in certain circumstances. Telephone numbers relate to telephones or other communications devices, IP addresses to computers, and street addresses to houses, rather than individuals, but such

---

23 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

information may come to be associated with a particular individual as information accretes around the number or address.

71.23 The ALRC also notes that while 'personal affairs' is generally considered to be a narrower concept than 'personal information',[24] Part 13 refers only to the 'affairs' of another person. It is arguable that 'affairs' relates to a broader category of information than 'personal affairs'. Further, Part 13 protects the information of 'persons' which includes organisations as well as individuals.[25] Therefore the 'affairs' of another person would cover types of information other than 'personal information', such as business affairs.

71.24 Part 13 also protects 'personal particulars'. Section 276 of the *Telecommunications Act* provides that 'personal particulars' includes 'any unlisted telephone number or any address'. In the ALRC's view, 'personal particulars' is potentially a broad category of information, and would cover 'personal information' where this information was held or collected for inclusion in a record and was about an individual whose identity was apparent, or could reasonably be ascertained.

71.25 In the interest of consistency and clarity, the ALRC sees merit in Part 13 generally referring to 'personal information'. It is the ALRC's view, however, that the information or documents protected under Part 13 would already include 'personal information'. Further, the ALRC has not consulted widely on this issue and is concerned that such an amendment could have unforeseen consequences.

71.26 In Chapter 72, however, the ALRC recommends the amendment of the *Telecommunications Act* to provide for direct marketing to existing customers of a telecommunications service provider. In the interest of consistency with the 'Direct Marketing' principle, this provision refers to 'personal information' as defined in the *Privacy Act*.

71.27 The ALRC also recommends the amendment of s 289(1)(b)(i) of the *Telecommunications Act* to protect 'sensitive information' as defined in the *Privacy Act*. Section 289(1)(b)(i) provides that the use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person, and the other person is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned. In the ALRC's view, such an amendment is appropriate to protect 'sensitive information' in the context of a very broad exception.

---

24 See discussion in Ch 15.

25 *Telecommunications Act 1997* (Cth) s 7.

Use and disclosure of information

71.28 NPP 2 and Part 13 of the *Telecommunications Act* regulate the use and disclosure of personal information. An organisation that uses or discloses personal information in a way that is authorised under the *Telecommunications Act* will not be in breach of NPP 2. An act or practice engaged in pursuant to any of the exceptions under Part 13 is an act or practice that is 'authorised by or under law' for the purposes of NPP 2 and the 'Use and Disclosure' principle in the model Unified Privacy Principles (UPPs).[26] This is confirmed by s 303B of the *Telecommunications Act*, which provides that a use or disclosure permitted under that Act is a use or disclosure that is 'authorised by law' for the purposes of the *Privacy Act.*[27]

71.29 Conversely, if a participant in the telecommunications industry engages in an act or practice that does not comply with one of the exceptions under Part 13, the act or practice would not be 'authorised by or under law', and may breach NPP 2 and the 'Use and Disclosure' principle.[28] This position is supported by s 303C of the *Telecommunications Act*, which provides that a prosecution for an offence relating to the use or disclosure of protected information under the *Telecommunications Act* does not prevent civil proceedings or administrative action being taken under the *Privacy Act* for the same breach.[29]

71.30 There is some uncertainty whether the exceptions under Part 13 provide the *only* circumstances in which it is lawful for those regulated by the *Telecommunications Act* to use or disclose that information. In particular, it is unclear whether the 'required or authorised by or under law' exception in s 280 of the *Telecommunications Act* allows the exceptions under NPP 2 in the *Privacy Act* to apply to the information protected under Part 13. This issue is discussed in detail in Chapter 72.

Other aspects of information handling

71.31 The *Privacy Act*, and in particular the NPPs, continue to regulate many aspects of the handling of personal information by telecommunications service providers. For example, a telecommunications provider only can collect personal information that is necessary for one or more of its functions or activities, such as to enable the provision of telecommunication services to a customer and to facilitate the billing for those services.[30] In addition, a telecommunications provider must take reasonable steps to ensure that an individual is aware of certain matters at or around the time of collection,

---

26 See Ch 22.
27 *Telecommunications Act 1997* (Cth) s 303B.
28 An act or practice that is prohibited under the *Telecommunications Act* may appear to be permitted under one of the other exceptions to NPP 2. This does not permit the act or practice, however, as Part 13 still applies to the use or disclosure of that information.
29 *Telecommunications Act 1997* (Cth) s 303C.
30 *Privacy Act 1988* (Cth) sch 3, NPP 1.1.

such as the types of organisations to which the provider usually discloses the information.[31]

Are two privacy regimes necessary?

71.32 A threshold question is whether two privacy regimes are necessary in the telecommunications industry, or whether the industry should be regulated under telecommunications-specific privacy laws or the *Privacy Act*.

Submissions and consultations

71.33 Some stakeholders argued that telecommunications-specific privacy laws are necessary. Stakeholders noted that Part 13 of the *Telecommunications Act* and the *Privacy Act* have different purposes. While the *Privacy Act* sets out individuals' rights relating to the handling of their personal information, Part 13 is directed more towards deterrence and punishment.[32]

71.34 Stakeholders also noted that Part 13 deals with many aspects of the telecommunications industry that are not addressed by the *Privacy Act*. For example, the Department of Communications, Information Technology, and the Arts (DCITA)[33] submitted that the content and substance of communications and unlisted numbers require industry-specific privacy regulation because they will not always be protected under the *Privacy Act*.[34]

71.35 Some stakeholders noted that while the *Privacy Act* is largely premised on organisations collecting personal information from an individual, this is not the case in the telecommunications industry. It was noted that the very nature of telecommunications carriage services necessitates carriage service providers receiving, not necessarily 'collecting', and disclosing information relating to the affairs and personal particulars of customers and people who are not their customers.[35]

71.36 It also was noted that the telecommunications industry has access to vastly more information about individuals than most organisations, including information about their own customers and other members of the general public. Such information includes the content of their communications. [36]

---

31 Ibid sch 3, NPPs 1.3, 1.5.

32 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Australian Federal Police, *Submission PR 186*, 9 February 2007.

33 Now the Department of Broadband, Communications and the Digital Economy.

34 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007.

35 I Graham, *Submission PR 427*, 9 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

36 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

71.37 The Office of the Victorian Privacy Commissioner (OVPC) submitted that telecommunications regulation is an area where fragmentation is a positive thing.

> Care should be taken not to ask or expect all things from generic privacy laws or from a single regulator. Here, separate regulation with purpose-built protections is desirable as it covers intrusive activities (eg listening in to telephone conversations) that may not generate any records. Privacy legislation is essentially about protecting documents or records, not transmissions.[37]

71.38 It was submitted that the *Telecommunications Act* permits the use and disclosure of personal information where it is necessary for the efficient functioning of the telecommunications industry. For example, the telecommunications sector relies on the interconnection of different telecommunication networks in order to enable a consumer to communicate with any other user, regardless of the networks to which those end-users are connected. Accordingly, exceptions under Part 13 of the *Telecommunications Act* that go beyond those available under the *Privacy Act* are necessary to enable industry networking arrangements to work efficiently and effectively.[38]

71.39 Other stakeholders, however, argued that much of the information used and disclosed in the telecommunications industry could be regulated under the *Privacy Act*. It was submitted that, in most cases, the personal information collected by telecommunications service providers is no different to personal information collected in other sectors. This information often will be obtained in the course of business but will not be related directly to the carriage of telecommunications services.[39] For example, personal information held by a telecommunications company, a bank or an electricity supplier in relation to any given customer is likely to be broadly similar—it would include identifying information such as the individual's name, address, telephone number and other contact information; as well as other information such as billing history, credit card details and likely income level.[40]

71.40 A number of stakeholders also noted that, due to technological and market 'convergence',[41] the boundaries between the telecommunications industry and other related industries are starting to blur.

> Increasingly, communications and related services will rely on a range of intermediate services and databases. If differences in the treatment of personal information persist

---

37 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007. See also Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007.

38 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007.

39 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

40 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007.

41 'Convergence' refers to a range of different technologies performing similar tasks. An example of a 'convergent device' is the mobile phone and other mobile communications devices that can act as multimedia platforms and, in particular, deliver audiovisual content. See Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 21; Australian Government Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006).

> between 'telecommunications' services and other businesses, the potential for unintended outcomes and for difficulties in administration across regulatory boundaries will increase markedly. This will become increasingly problematic as communications becomes embedded in more and more services.[42]

71.41 The communications industry also is experiencing business diversification, specialisation and the entry of new niche industry participants. The lower cost of creating and distributing digitalised content and communications is lowering barriers to market entry and resulting in the emergence of new online services and environments.[43]

71.42 Stakeholders outlined a number of options for reform. It was suggested in one submission that the development of an instrument focused on telecommunications privacy would be appropriate.[44] The European Union has taken steps to regulate specifically the handling of data by the telecommunications industry. For example, the 2002 Directive on privacy and electronic communications requires Member States to enact legislation to ensure the confidentiality of telecommunications and telecommunications data,[45] and to ensure that subscribers to telecommunication services are given the opportunity to determine whether their personal data are included in a public directory.[46] The 2006 data retention Directive aims to ensure that telecommunications data are retained for a certain period in case they are required for law enforcement purposes.[47] It also requires Member States to ensure that data are stored securely, and destroyed at the end of the retention period.[48]

71.43 Another stakeholder argued that the deregistration of the ACIF *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* has resulted in regulatory gaps in the protection of personal information in the telecommunications industry. It also was noted that deregistration of the Code has resulted in a number of small telecommunications businesses not being regulated by any privacy rules, as they are not covered by the *Privacy Act*.[49] AAPT suggested that one option would be the development of an overarching document, whether a code, guide or separate piece of legislation, that provides a comprehensive overview of telecommunications privacy.[50] Others submitted, however, that the development of a

---

42 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007. See also Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

43 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 22.

44 K Pospisek, *Submission PR 104*, 15 January 2007.

45 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002), art 5.

46 Ibid, art 12.

47 European Parliament, *Directive on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks*, Directive 2006/24/EC (2006), art 1.

48 Ibid, art 7.

49 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

50 AAPT Ltd, *Submission PR 87*, 15 January 2007.

telecommunications-specific industry privacy code is likely to result in additional compliance cost and a greater overlap with existing regulation.[51]

71.44 The OPC submitted that consideration should be given to removing the exceptions under Part 13 (while keeping the Part 13 offence provisions), and allowing the *Privacy Act* to regulate use and disclosure under that Part.[52]

71.45 It was also suggested that Part 13 could be moved into the *Privacy Act*, perhaps as an industry-specific section of the Act.[53] Optus submitted that telecommunications privacy provisions, if included in the *Privacy Act*, should:

- cover both personal information, including the affairs or personal particulars of persons, as well as the content of communications and carriage services;
- contain the same protections regarding the primary and secondary uses and disclosures contained within the *Telecommunications Act*; and
- contain the exemptions from Part 13 of the *Telecommunications Act* that cover the permitted use and disclosure of content, carriage services and personal information.[54]

71.46 Stakeholders also suggested that privacy regulation applying to the telecommunications sector should be aligned with the general privacy provisions contained in the *Privacy Act*, particularly in the area of exemptions and penalties.[55] The OPC Review noted the possibility of amending the *Telecommunications Act* and the *Privacy Act* to ensure the highest of the two standards always operates.[56]

ALRC's view

71.47 The ALRC sees merit in the promulgation of telecommunications privacy regulations under the *Privacy Act* to regulate the handling of personal information. The regulations could:

- protect 'personal information' regardless of whether the information came into the knowledge or possession of a telecommunication services provider in the circumstances outlined in Part 13;

---

51 Telstra, *Submission PR 185*, 9 February 2007.

52 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

53 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

54 Optus, *Submission PR 532*, 21 December 2007.

55 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

56 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 60.

- contain the same protections regarding the primary and secondary uses and disclosures contained within the *Telecommunications Act*; and

- contain the exemptions from Part 13 of the *Telecommunications Act* that cover the permitted use and disclosure of content, carriage services and personal information.

71.48 Another option would be for the Privacy Commissioner to issue binding telecommunications privacy guidelines similar to the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* (Medicare Guidelines) issued under s 135AA of the *National Health Act 1953* (Cth).[57] The advantage of both these options is that the telecommunications industry would have one set of rules to regulate the handling of 'personal information' and possibly other information.[58]

71.49 The ALRC has concluded, however, that both the *Telecommunications Act* and the *Privacy Act* should continue to regulate privacy in the telecommunications industry. The ALRC has reached this conclusion based on a number of considerations.

71.50 First, the telecommunications industry handles sensitive personal information. In addition to financial information, telephone numbers and other contact information, telecommunications service providers hold information about when, how and with whom individuals communicate, and the content of those communications. It is appropriate that the use and disclosure of this information is subject to more stringent rules than those in the *Privacy Act*.

71.51 The ALRC acknowledges that other organisations, such as banks, handle information that is just as sensitive as information handled by telecommunications service providers, and that these organisations are not regulated under stringent provisions such as Part 13 of the *Telecommunications Act*. The ALRC notes, however, that banks and other financial institutions are subject to a range of laws other than the *Privacy Act* that regulate the handling of sensitive financial information.[59] Further, organisations and agencies that handle particularly sensitive information are often subject to secrecy provisions that are more stringent than the *Privacy Act* provisions. These provisions are discussed in Chapter 15.

---

57 Office of the Privacy Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs: Issued under Section 135AA of the National Health Act 1953* (2008).

58 The ALRC notes that the Medicare Guidelines regulate 'Medicare claims information' and 'Pharmaceutical Benefits claims information'. This information would include information other than 'personal information' as defined in the *Privacy Act 1988* (Cth): Office of the Privacy Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs: Issued under Section 135AA of the National Health Act 1953* (2008).

59 These laws include the common law duty of confidence owed by banks to their customers (see discussion in Ch 53) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (see discussion in Ch 16).

71.52 Secondly, as outlined above, the *Telecommunications Act* protects a broader category of information than the *Privacy Act* in the context of information that comes into the knowledge or possession of a person in the circumstances outlined in Part 13. For example, the *Privacy Act* regulates only personal information held or collected for inclusion in a 'record'.[60] In contrast, Part 13 of the *Telecommunications Act* regulates information that may or may not be held in a record.[61] Further, Part 13 of the *Telecommunications Act* regulates information and documents about organisations, as well as individuals.[62]

71.53 The ALRC considered whether Part 13 should be transferred to the *Privacy Act*. The ALRC also considered whether the *Privacy Act* or the *Telecommunications Act* should regulate 'personal information' handled by telecommunications service providers regardless of whether it came into their knowledge or possession in the circumstances outlined in Part 13. Such an amendment, however, would create confusion and further fragment the regulation of the telecommunications industry. Further, as noted above, it is the ALRC's view that the type and volume of information handled by telecommunications service providers warrants special protection.

71.54 Thirdly, Part 13 of the *Telecommunications Act* does not regulate all stages of the information-handling cycle. These matters are dealt with under the *Privacy Act*. The ALRC considered whether Part 13 of the *Telecommunications Act* should be amended to include rules relating to all stages of the information-handling cycle. The ALRC concluded, however, that because Part 13 regulates, in addition to personal information, the handling of non-personal information, such an amendment could create further complexity, may not be appropriate in the context of non-personal information, and may be beyond the ALRC's Terms of Reference for this Inquiry.

71.55 Fourthly, the ALRC notes that specific exceptions to the offence provisions in Part 13, which go beyond those available under the *Privacy Act*, are necessary to enable industry networking arrangements to work efficiently and effectively. The ALRC considered whether telecommunications-specific exceptions under the *Privacy Act* could accommodate these uses and disclosures. In the ALRC's view, however, this would add an undesirable layer of complexity to privacy regulation in the telecommunications industry. The exceptions to the use and disclosure offences are considered in Chapter 72.

71.56 Finally, determining whether a telecommunications service provider has complied with Part 13 requires technical knowledge and understanding of how the telecommunications industry operates. The *Telecommunications Act* is currently administered by ACMA. ACMA has expertise in the regulation of the telecommunications industry that the OPC does not have.

---

60 *Privacy Act 1988* (Cth) s 16B. 'Record' is defined under s 6 of the *Privacy Act 1988* (Cth).

61 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

62 For example, Part 13 regulates the use and disclosure of the affairs 'of another person'. 'Person' is defined in s 7 of the *Telecommunications Act* as including a partnership.

71.57 The interaction between the *Telecommunications Act* and the *Privacy Act* should be clarified. The ALRC's approach to reform in this area involves:

- clarification of the scope of the exceptions to the use and disclosure offences under the *Telecommunications Act*;
- where appropriate, the alignment of the exceptions to the use and disclosure offences under the *Telecommunications Act* with the exceptions under the 'Use and Disclosure' principle in the model UPPs;
- ensuring that all participants in the telecommunications industry are subject to privacy regulation;
- the development and publication of guidance relating to privacy in the telecommunications industry that addresses the interaction between the *Telecommunications Act* and the *Privacy Act*; and
- greater cooperation between the bodies with responsibility for privacy regulation in the telecommunications industry.

A redraft of the Part

71.58 In Discussion Paper 72, *Review of Australian Privacy Law* (DP 72), the ALRC noted that AAPT had submitted that it is sometimes difficult to understand the requirements of Part 13 of the *Telecommunications Act*, and that this creates additional confusion in an area already complicated by the proliferation of legislation and regulation.[63] The ALRC proposed that Part 13 of the *Telecommunications Act* should be redrafted to achieve greater logical consistency, simplicity and clarity.[64]

71.59 A number of stakeholders supported the proposal.[65] Communications Alliance submitted that Part 13 of the *Telecommunications Act* should be redrafted as part of an overall review of telecommunications sector legislation.[66] The Australian Privacy Foundation supported a redraft of Part 13 provided that it was not used as an excuse for not proceeding with some urgently needed amendments.[67]

---

63 AAPT Ltd, *Submission PR 87*, 15 January 2007.

64 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–14.

65 Optus, *Submission PR 532*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

66 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

67 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

71.60 In the ALRC's view, Part 13 should be redrafted to achieve greater logical consistency, simplicity and clarity. As discussed in Chapter 72, the scope of a number of the provisions is unclear—particularly the exceptions to the use and disclosure offences. Part 13 does not follow a logical structure. For example, the exceptions to the use and disclosure offences are separated by the provisions relating to Integrated Public Number Database (IPND) authorisations. Finally, the provisions relating to the relationship between Part 13 and the *Privacy Act* should be located earlier in the Part.

Recommendation 71–1 Part 13 of the *Telecommunications Act 1997* (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.

A review of telecommunications regulation

71.61 The ALRC acknowledges the need for telecommunications regulation to respond to a convergent communications environment. This has been a theme in a number of recent reports and inquiries.[68] In Australia, there are currently a number of regulatory frameworks that apply to information according to the communications platform over which it is delivered.[69]

71.62 In DP 72, the ALRC expressed the view that issues related to convergence extend beyond the Terms of Reference for this Inquiry. The ALRC proposed, therefore, that the Australian Government should initiate a review to consider the extent to which the *Telecommunications Act* and the *Telecommunications (Interception and Access) Act*[70] continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries, and changing community perceptions and expectations about communication technologies.[71]

---

68 See, eg, Australian Government Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006); Australian Communications Authority, *Vision 20/20: Future Scenarios for the Communications Industry—Implications for Regulation* (2005).

69 See, eg, *Telecommunications Act 1997* (Cth); *Broadcasting Services Act 1992* (Cth).

70 The *Telecommunications (Interception and Access) Act 1979* (Cth) is discussed in Ch 73.

71 In particular, the ALRC proposed that the review should consider: whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services; how the Acts interact with each other and with other legislation; the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation; and the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including ACMA, the Australian Government Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance: Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–1.

Submissions and consultations

71.63 A number of stakeholders supported such a review.[72] Communications Alliance supported a review, but noted that it should form part of a much larger review of Australia's 'broadband future'. The Alliance submitted that the Government should consider developing a comprehensive framework of legislative and administrative measures that are 'purpose built for the broadband world, and not bolted on to the legacy tools of the pre-digital era'.[73]

71.64 Telstra supported a review, but noted that it should commence after the completion of the ALRC's Inquiry and cover other telecommunications legislation, such as the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).[74] National Legal Aid submitted that the review should cover the use of telecommunications data by state and territory law enforcement agencies, having regard to the lack of uniform coverage for state law enforcement agencies under privacy laws.[75] The Australian Direct Marketing Association and Communications Alliance submitted that it is fundamentally important that all telecommunications stakeholders are consulted as part of a review. [76]

71.65 Some stakeholders opposed the proposal for a review. The Department of Broadband, Communications and the Digital Economy (DBCDE) submitted that such a review would need to consider a much wider range of issues than privacy, and that the implications of the ALRC's proposal go well beyond the scope of the ALRC's Inquiry. In the DBCDE's view, it would be outside the ALRC's Terms of Reference to recommend such a review.[77] Other stakeholders noted that it is important that such legislation is kept under constant review, and questioned the need for a review given recent reviews of the legislation.[78]

71.66 The Attorney-General's Department noted that while convergence raises a number of issues for the *Telecommunications (Interception and Access) Act* and law enforcement agencies, the technology-neutral language of the legislation has allowed the Act to remain effective in its application, and agencies to work together to address convergence issues as they arise.[79]

---

72 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

73 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

74 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

75 National Legal Aid, *Submission PR 521*, 21 December 2007.

76 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

77 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007. See also Optus, *Submission PR 532*, 21 December 2007.

78 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; Australian Federal Police, *Submission PR 545*, 24 December 2007.

79 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

ALRC's view

71.67 Issues related to convergence extend beyond the Terms of Reference for this Inquiry. In the ALRC's view, the Australian Government should initiate a review of telecommunications regulation in the light of technological developments (including technological convergence), changes in the structure of communication industries and shifting community perceptions and expectations about communication technologies.[80] This review should consider other legislation that regulates the telecommunications industry and how it interacts with the *Telecommunications Act.*[81]

71.68 A recommendation for such a review is clearly within the ALRC's Terms of Reference. As noted above, the then Attorney-General, the Hon Philip Ruddock MP, specifically asked the ALRC to consider the interaction between the *Privacy Act* and Part 13 of the *Telecommunications Act* during the course of this Inquiry. The need for such a review has become evident as a result of the ALRC's review of Part 13. Further, a recommendation for such a review falls within the ALRC's Terms of Reference for this Inquiry which require the ALRC to consider 'any other related matter'.

71.69 The ALRC notes that some aspects of this legislation have been reviewed relatively recently. Recent reviews have focused on specific areas of telecommunications regulation. In the ALRC's view, regulation of telecommunications more broadly should be reviewed. The ALRC notes that the amalgamation of key broadcasting and telecommunications regulators in the United Kingdom provided the opportunity to establish a new regulatory framework under the *Communications Act 2003* (UK).

71.70 The ALRC recommends, therefore, that the review should consider the extent to which the activities regulated under the *Telecommunications Act* and the *Telecommunications (Interception and Access) Act* should be regulated under general communications legislation or other legislation; and the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including ACMA, the Attorney-General's Department, the OPC, the Telecommunications Industry Ombudsman (TIO), and Communications Alliance.

71.71 The establishment of a public interest monitor (PIM) should be considered as part of the recommended review. In Chapter 73, the ALRC considers whether the *Telecommunications (Interception and Access) Act* should provide for the role of a PIM to oversee the interception and access of communications. The ALRC does not recommend the establishment of a PIM because many of the functions of a PIM are adequately provided by other bodies. The ALRC acknowledges, however, that most of these functions occur after a warrant has been issued or the interception or access of communications.

---

80 Senate Environment Communications Information Technology and the Arts References Committee, *A Lost Opportunity? Inquiry into the Provisions of the Australian Communications and Media Authority Bill 2004 and Related Bills and Matters* (2005), rec 1.

81 The *Telecommunications (Interception and Access) Act 1979* (Cth) is discussed in Ch 73.

Recommendation 71–2 The Australian Government should initiate a review to consider whether the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how these two Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and

(e) whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a public interest monitor.

Does the *Telecommunications Act* provide adequate privacy protection?

71.72 In DP 72, the ALRC considered whether the *Telecommunications Act* provides adequate and effective protection for the use, disclosure and storage of personal information. The ALRC noted that, while one stakeholder submitted that the *Telecommunications Act* operates effectively in tandem with the *Privacy Act*,[82] other stakeholders raised a range of issues related to telecommunications privacy regulation including: confusion about how the two Acts interact; regulatory gaps caused by the small business exemption; the impact of new privacy-invasive technologies; and the role and function of the various bodies with responsibility for telecommunications privacy. These issues are addressed below.

82 Telstra, *Submission PR 185*, 9 February 2007.

71.73 Stakeholders also noted the lack of clarity around the exceptions to the use and disclosure offences and suggested that there is inadequate protection of personal information held on public number directories. These issues are discussed in Chapter 72.

Small business exemption

71.74 The *Privacy Act* generally does not apply to businesses with an annual turnover of $3 million or less.[83] Telecommunications service providers in this category, however, are obliged to comply with Part 13 of the *Telecommunications Act*. As discussed above, Part 13 only regulates the use and disclosure of information. It does not regulate other aspects of the information-handling cycle, such as the collection and storage of personal information.[84]

71.75 In addition, some organisations that are closely associated with the telecommunications industry may not fall under Part 13 of the *Telecommunications Act* or the *Privacy Act*. For example, directory assistance providers that are not carriage service providers, and some voice over internet protocol service providers may not be subject to Part 13 of the *Telecommunications Act*, an industry code, or the *Privacy Act*.

71.76 In DP 72, the ALRC noted that the development of communications technologies and e-commerce has resulted in more businesses, particularly small to medium businesses, handling large amounts of personal information.[85] A number of stakeholders submitted that, given the high proportion of small businesses in the telecommunications industry, it was not appropriate to treat them differently from medium and large businesses.[86]

71.77 The OPC submitted that there are certain activities that should be regulated because of the nature of the activity, rather than the size of the organisation. The OPC suggested that carriage service providers and internet service providers (ISPs) fall into this category because of the amount of personal information they hold, and the potential adverse impact on individuals if that information is not protected appropriately.[87]

---

83 *Privacy Act 1988* (Cth) ss 6C, 6D. Businesses with an annual turnover of $3 million or less, however, are bound by the NPPs in certain circumstances such as when the business discloses personal information about another individual for a benefit, service or advantage: see *Privacy Act 1988* (Cth) s 6D(4).

84 Many of these providers were formerly subject to obligations similar to those imposed by the NPPs under the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999). However, this code was repealed when the private sector provisions of the *Privacy Act* commenced in December 2001: see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 56.

85 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [63.151].

86 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007; Law Society of New South Wales, *Submission PR 146*, 29 January 2007; Confidential, *Submission PR 31*, 3 June 2006.

87 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

71.78 Communications Alliance recommended, however, that education and awareness raising and incentives to industry for voluntary adoption of the NPPs would solve the problem. The organisation did not support additional codes which would increase the regulatory burden on small businesses.[88]

71.79 In DP 72, the ALRC proposed that before the removal of the small business exemption from the *Privacy Act* comes into effect, the Australian Government should make regulations under s 6E of the *Privacy Act* to ensure that the Act applies to all small businesses in the telecommunications industry, including internet service providers and public number directory producers.[89] A number of stakeholders supported this proposal.[90]

ALRC's view

71.80 The risks to privacy posed by small businesses are determined by the amount and nature of personal information held, the nature of the business and the way personal information is handled by the business, rather than by their size alone. The ALRC notes that the telecommunications industry is increasingly handling large amounts of personal information. It is appropriate that the handling of personal information by these organisations is regulated by the *Privacy Act*.

71.81 In Chapter 39, the ALRC recommends the removal of the small business exemption.[91] The implementation of this recommendation would solve the problem of some small businesses in the telecommunications industry not being subject to any privacy rules. It is therefore unnecessary for the Australian Government to make regulations under s 6E of the *Privacy Act* to ensure that the Act applies to all small businesses in the telecommunications industry. The recommended review, however, should consider whether these organisations should be regulated under telecommunications-specific laws, such as Part 13 of the *Telecommunications Act* or the *Privacy Act*.

71.82 Education has an important role to play in securing compliance with privacy standards. The ALRC acknowledges concerns about the additional compliance burden for small business if they are required to comply with the *Privacy Act*. In Chapter 39, the ALRC discusses ways to reduce the compliance burden on small businesses, including: the establishment of a national helpline for small businesses; the development and publication of guidelines and other educational material by the OPC

---

88 Communications Alliance Ltd, *Submission PR 198*, 16 February 2007.

89 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–10.

90 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Australian Digital Alliance, *Submission PR 422*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007.

91 Rec 39–1.

to assist small businesses; and the provision of templates for Privacy Policies free of charge.

Criminal or civil penalties?

71.83 A criminal penalty is the only remedy available for a breach of the use and disclosure offences under Part 13 of the *Telecommunications Act*. For example, s 276 provides that a person who contravenes that section is guilty of an offence punishable by imprisonment for a term not exceeding two years. Criminal offences, whether in statute or common law, are considered to be made up of physical and mental elements, also described as the prohibited act (*actus reus*) and the criminal mental element (*mens rea*). The mental element for the primary and secondary disclosure offence provisions under Part 13 is 'intention'.[92]

71.84 In a regulatory context, criminal sanctions serve as a last-resort punishment after repeated or wilful violations. [93] There have been no prosecutions for breaches of the prohibitions under Part 13 since the *Telecommunications Act* was enacted. In DP 72, the ALRC asked whether a breach of Divisions 2, 4 and 5 of Part 13 of the *Telecommunications Act* should attract a civil penalty rather than a criminal penalty.[94]

71.85 Civil penalty provisions are founded on the notion of preventing or punishing public harm. The contravention itself may be similar to a criminal offence and may involve the same or similar conduct, and the purpose of imposing a penalty may be to punish the offender, but the procedure by which the offender is sanctioned is based on civil court processes. Civil monetary penalties play a key role in regulation as they may be sufficiently serious to act as a deterrent (if imposed at a high enough level) but do not carry the stigma of a criminal conviction. Civil penalties may be more severe than criminal penalties in many cases.[95]

Submissions and consultations

71.86 A number of stakeholders supported a breach of Divisions 2, 4 and 5 of Part 13 attracting civil penalties rather than criminal penalties.[96] For example, the Australian Privacy Foundation submitted that:

> in our view breaches of the privacy protection provisions of the *Telecommunications Act* should attract civil rather than criminal penalties—the lower burden of proof is

92 *Criminal Code* (Cth) s 5.6(1).

93 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.40]–[2.44].

94 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–6.

95 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.40]–[2.44].

96 Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

> appropriate. The level of civil penalties must however be sufficient to act as a significant deterrent to calculated non-compliance.[97]

71.87 ACMA submitted, however, that civil penalties, in addition to criminal penalties, may assist it in better ensuring compliance with the requirements of Part 13 in a self-regulatory environment.[98] The DBCDE submitted that, given that the offences in Part 13 apply to organisations and their employees, both criminal offences and civil penalties should apply to provide the maximum flexibility to deal with particular cases.[99]

ALRC's view

71.88 The *Telecommunications Act* should be amended to provide that a breach of Divisions 2, 4 or 5 of Part 13 of the Act may attract a civil penalty or a criminal penalty.

71.89 The ALRC has concluded that criminal penalties continue to be justified for the intentional use and disclosure of information or documents obtained during the supply of telecommunications services. As noted above, this information is highly sensitive, and includes information about when, how and with whom individuals communicate. Individuals expect a high level of protection of this information or documents relating to their use of telecommunications services. The intentional use and disclosure of this information in contravention of Part 13 so seriously offends this expectation that criminal penalties are justified to deter and punish such conduct. Further, the current regime appears to be working effectively. The ALRC notes that there have been no prosecutions for breaches of the prohibitions under Part 13 since the *Telecommunications Act* was enacted.

71.90 The Attorney-General's Department publication, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (the Guide), states that it is important that civil penalties be used in appropriate and justifiable contexts. Civil penalties are otherwise open to criticism for being too soft (in not carrying a criminal penalty) or for being too harsh (in not carrying the safeguards of criminal procedure such as a requirement for proof beyond reasonable doubt).[100]

71.91 The Guide provides that the inclusion of civil penalty provisions is most likely to be appropriate and effective where each of the following circumstances is present:

- Criminal punishment is not merited. Only contraventions of the law involving serious moral culpability should be pursued by criminal prosecution. Offences

---

97 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also I Graham, *Submission PR 427*, 9 December 2007.

98 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

99 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

100 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), [7.2].

involving harm to a person or a serious danger to public safety or knowing or reckless dishonesty by a person are examples.

- The penalty is sufficient to justify court proceedings. A contravention should be punishable by civil penalty only if the size of the maximum penalty will justify the expense and time required to take the matter to court.

- There is corporate wrongdoing. Civil penalties have traditionally been directed against corporate wrongdoing where imprisonment is not available (because the wrongdoing is by a corporate entity). In this case, the financial disincentive that civil penalties provide is most likely to be useful and effective.[101]

71.92 The inclusion of civil penalties in Part 13 of the *Telecommunications Act* is appropriate and justifiable in each of the circumstances outlined above. Further, the introduction of civil penalties into the *Telecommunications Act* will provide ACMA with a greater range of options for enforcing the Act when contraventions fall short of a criminal offence.

71.93 The introduction of civil penalties in addition to criminal penalties raises the issue of how a contravention attracting a civil penalty should be distinguished from an offence that attracts a criminal penalty. The Guide states that it is acceptable to have the same physical elements covered by both civil penalties and criminal sanctions where culpability differs.[102]

71.94 A number of provisions under federal regulatory laws provide for parallel criminal liability and civil penalties for the same conduct.[103] Under this model criminal or 'offence' provisions generally require proof to a criminal standard (beyond reasonable doubt) of physical elements and certain fault elements (usually intention or recklessness). Civil penalty provisions may require proof of the same physical elements to a civil standard (on the balance of probabilities), however, they often do not require proof of any fault elements.

71.95 This model is appropriate in the context of Part 13 of the *Telecommunications Act*. Under this model, the requirement to prove intention will distinguish criminal liability from civil liability. Intention therefore will only need to be proven when a criminal penalty is considered to be appropriate in the circumstances.

71.96 The introduction of civil penalties into Part 13 of the *Telecommunications Act* will require the introduction of a number of additional procedural provisions. For example, provisions should be introduced to ensure that an order imposing a civil

---

101 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), [7.2].

102 Ibid, [7.2].

103 Examples appear in the *Corporations Act 2001* (Cth), the *Environmental Protection and Biodiversity Conservation Act 1999* (Cth) and the *Commonwealth Authorities and Companies Act 1997* (Cth).

penalty is not made against a person where the person has been convicted of an offence constituted by conduct that is substantially the same as the conduct constituting the contravention. It is analogous to the 'double jeopardy' rule applicable to criminal offences.[104] The Guide sets out a number of other procedural provisions that will be relevant if civil penalties are introduced into Part 13 of the *Telecommunications Act*.[105]

71.97 As noted in *Principled Regulation: Federal Civil and Administrative Penalties in Australia* (ALRC 95), the choice of criminal or civil penalty proceedings calls for transparency in the application of discretions.

> The availability of this choice can lead to uncertainty both for regulators and the regulated, and it has the potential to lead to inconsistency in the regulator's approach to commencing proceedings. Care must be taken that the reasons that a criminal prosecution is commenced against one offender while another faces 'only' civil penalty proceedings are transparent and consistent. Difficulties in proving the mental elements of the offence to the criminal standard may well be the reason for the decision to take proceedings for a civil penalty in one case, while in another, it may be that the breach lacked the requisite fault.[106]

71.98 The ALRC recommends that ACMA should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil or a criminal penalty is made. Enforcement guidelines have a number of benefits including improving the understanding of the regulated community as to what compliance requires; and greater accountability, transparency and consistency of regulators' decisions.[107] Enforcement guidelines are discussed in detail in Chapter 50.

Recommendation 71–3 The *Telecommunications Act 1997* (Cth) should be amended to provide that a breach of Divisions 2, 4 and 5 of Part 13 of the Act may attract a civil penalty in addition to a criminal penalty. The Australian Communications and Media Authority should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil or a criminal penalty is made.

104 See, eg, *Environmental Protection and Biodiversity Conservation Act 1999* (Cth) s 486C.

105 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), [7.4].

106 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [4.69].

107 Ibid, [10.60].

New technologies

71.99 This section considers briefly three relatively new technologies that are considered to have privacy implications—voice over internet protocol (VoIP), electronic numbering (ENUM) and web server logs. These technologies are also discussed in Part B.

Voice over internet protocol

71.100 VoIP enables spoken conversations to be conducted in real time over the internet. VoIP services usually operate over a telecommunications network and are classified as carriage services for the purposes of the *Telecommunications Act*.[108] This means that VoIP service providers generally will be 'carriage service providers' that are required to observe the provisions in Part 13 of the *Telecommunications Act*.

71.101 There are also, however, a variety of VoIP products and services that are closer to pure internet applications in that they tend only to operate over internet protocol networks, and not the Australian Public Switched Telephone Network (PSTN).[109] For example, instant messaging products such as Yahoo Messenger and MSN Messenger allow voice communications from computer to computer over the internet. If a VoIP service does not connect with the PSTN at all, the service provider may not be regulated by the *Telecommunications Act* but may be regulated by the *Privacy Act*.[110] It has been noted that:

> The *Telecommunications Act* does not govern the use of these products and services, and it can be persuasively argued that it does not need to. Those who utilise VoIP products and services of this class have no expectations of a telephony-grade service—they would not, for example, be likely to attempt to make an emergency call using such a service … On the other hand, the privacy issues raised by the use of this class of VoIP products and services are no less real simply because they are not appropriate to be regulated by the *Telecommunications Act*.[111]

71.102 The OPC submitted that it is unclear whether the definition of a 'carriage service provider' in s 87 of the *Telecommunications Act* will always encompass the regulation of ISPs, where ISPs provide services that are similar to those of traditional carriage service providers (for example, where an ISP is hosting VoIP services, which are telephone call services that do not route through the regular PSTN).[112] In the ALRC's view, it is outside the Terms of Reference for the current Inquiry to consider whether the definition of 'carriage service provider' under s 87 of the

---

108 Australian Government Department of Communications, Information Technology and the Arts, *Examination of Policy and Regulation Relating to Voice Over Internet Protocol (VOIP) Services* (2005), 19.

109 The PSTN is the network of the world's public circuit-switched telephone networks. It was originally a network of fixed-line analog telephone systems, but is now almost entirely digital, and includes mobile as well as fixed telephones.

110 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 26.

111 Ibid, 26.

112 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

Telecommunications Act should be amended. This issue should be considered as part of the recommended review of the *Telecommunications Act*.[113]

71.103 Another concern that has arisen in relation to VoIP technology is that Australians may access voice services from providers outside Australia.[114] This may have an impact on the standards of protection for personal information disclosed during a VoIP call.[115] The OPC Review recommended that the Australian Government initiate discussions in international forums to deal with international jurisdictional issues arising from the global reach of new technologies such as VoIP.[116] The ALRC supports this recommendation.

ENUM

71.104 ENUM is an abbreviation for electronic numbering or electronic number mapping. ENUM is 'an electronic numbering system that can link the public telephone network and the internet by allowing telephone numbers to be converted into internet domain names'.[117] In summary, ENUM enables telephones connected to the internet to make calls to the PSTN and receive calls from the PSTN.[118] The ALRC notes that ACMA has completed a trial of ENUM.[119] It is not known if or when ENUM will become available in Australia.[120]

71.105 ACMA submitted that the next development in ENUM technology, infrastructure ENUM, will involve the mapping of blocks of ENUM registrations 'to a single Internet resource—generally a Voice over Internet Protocol (VoIP) address'.[121] One application of infrastructure ENUM could involve the 'peering'—or direct connection—of VoIP services in isolation from the PSTN.[122]

71.106 ACMA commissioned an independent privacy consultant to prepare a privacy impact assessment (PIA) for its ENUM project.[123] The Privacy Impact Assessment made 13 recommendations relating to the implementation of the ENUM project. These recommendations included that ACMA:

---

113 Rec 71–1.
114 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 25.
115 Ibid, 25.
116 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 70.
117 Australian Communications Authority, *Annual Report 2004–05* (2005), 36.
118 Australian Communications and Media Authority, *What is ENUM or Electronic Number Mapping?* <www.acma.gov.au> at 30 July 2007.
119 Australian Communications and Media Authority, *Australian ENUM News* (2006) <www.acma.gov.au/WEB/STANDARD//pc=PC_2328> at 30 April 2008.
120 ENUM is discussed in more detail in Chs 9, 10.
121 Australian ENUM Discussion Group, *Evaluation of the Australian ENUM Trial* (2007), App B; Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.
122 See, eg, Australian Communications and Media Authority, *Australian ENUM News* (2006) <www.acma.gov.au/WEB/STANDARD//pc=PC_2328> at 30 April 2008.
123 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

- adopt, as a guiding principle in relation to ENUM, the position that privacy protections must be no less than those affecting PSTN telephony now;

- ensure that ENUM providers do not request individuals' address details except as required for any billing purposes, in which case post office boxes should be acceptable;

- require ENUM providers to publish and maintain a Privacy Policy on their website; and

- ensure ENUM providers understand that registration cannot be made conditional upon customers giving 'consent' to any unrelated secondary uses or disclosures of their personal information. [124]

71.107 The ALRC understands that ACMA is in the process of implementing these recommendations.[125]

71.108 In the ALRC's view, it is too soon to recommend legislative amendment to accommodate ENUM in the *Privacy Act* or telecommunications-specific legislation. Further, as noted in Chapter 10, maintaining technology-neutral privacy legislation is the most effective way to ensure individual privacy protection in light of developing technology.

71.109 The public, however, should understand the privacy risks and issues associated with new technologies such as ENUM. The ALRC recommends below that ACMA, in consultation with relevant stakeholders, should develop and publish guidance that addresses privacy issues raised by new technologies such as ENUM.

Web server logs

71.110 Electronic Frontiers Australia noted that it is highly concerned that neither the *Privacy Act* nor the *Telecommunications Act* adequately protect personal information contained in web server logs and similar logs, due in part to an inadequate definition of 'personal information'. It considers that internet protocol addresses should be regarded as 'personal information' because they can be used to identify individuals.

> EFA considers legislative amendments are necessary as a matter of priority to prevent the disclosure of information about Internet users' web browsing activities on the grounds of claims that IP addresses are not personal information and that therefore disclosure and use is not regulated.[126]

71.111 The ALRC examines the definition of 'personal information' in Chapter 6. In that chapter, the ALRC notes that information that simply allows an individual to be

---

124 Australian ENUM Discussion Group, *Evaluation of the Australian ENUM Trial* (2007), App B.
125 Australian ENUM Discussion Group, *Evaluation of the Australian ENUM Trial* (2007), App B.
126 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

contacted—such as an internet protocol address—in isolation, would not fall within the definition of 'personal information'. The *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. Contact information, however, may become 'personal information', however, in certain contexts once an internet protocol address is linked to a particular individual.

71.112 The use and disclosure offences under Part 13 of the *Telecommunications Act* protect any information or document that relates to the 'affairs or personal particulars (including any unlisted telephone number or any address) of another person', the contents of communications or carriage services supplied by carriers and carriage service providers.[127] There is a strong argument that this information would include an internet protocol address.[128]

Guidance on new technologies

71.113 In DP 72, the ALRC expressed the view that the privacy impact of new communications technologies should be addressed in guidance and that this guidance should address not only compliance with the proposed UPPs, but also requirements under the *Telecommunications Act* and industry codes and standards. The ALRC proposed that ACMA, in consultation with the OPC, Communications Alliance and the TIO, should develop and publish guidance that addresses issues raised by new technologies such as location-based services, VoIP and ENUM.[129]

Submissions and consultations

71.114 A number of stakeholders supported the proposal.[130] Communications Alliance advised that it, along with ACMA, the OPC and the TIO, have agreed in principle to develop guidelines that address the impact of new technologies on privacy related issues. Communications Alliance noted that it would welcome the opportunity to draft an 'industry led solution', given its experience of working with the *Telecommunications Act*.[131]

71.115 Stakeholders noted that ACMA should consult with various bodies when developing the proposed guidance,[132] including law enforcement agencies,[133] consumer organisations,[134] and the DBCDE.[135] Optus submitted that such guidance is

---

127 See, eg, *Telecommunications Act 1997* (Cth) ss 276, 277.

128 See, eg, Replacement Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), 6.

129 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–11.

130 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

131 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

132 Australian Digital Alliance, *Submission PR 422*, 7 December 2007.

133 Australian Federal Police, *Submission PR 545*, 24 December 2007.

134 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

135 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

unnecessary because the application of the NPPs to new technologies was well understood.[136]

71.116 ACMA submitted that its educative functions might extend to the provision of information to the community about new technologies, and that it will consider factoring the development of such information into its programs, as the need arises. ACMA recommended, however, that Communications Alliance should be encouraged to develop guidelines for industry participants to conduct PIAs of emerging technologies, applications and services, such as location-based services, VoIP, and electronic number mapping initiatives.[137]

ALRC's view

71.117 In Chapter 10, the ALRC suggests that making the *Privacy Act* technology neutral is the most effective way to ensure individual privacy protection in light of developing technology. Current technologies do not alter fundamentally the nature of the information-handling cycle. The ALRC notes the limitations of the *Telecommunications Act* in dealing with converging technologies in the telecommunications environment.

71.118 ACMA, in consultation with the OPC, Communications Alliance and the TIO, should develop and publish guidance that addresses issues raised by new technologies. This guidance should provide advice on compliance with the model UPPs and requirements under the *Telecommunications Act*, industry codes and standards. ACMA should be required to consult broadly with industry stakeholders, including consumer groups, law enforcement agencies, government departments, and industries that may use such technologies.

71.119 ACMA, in consultation with the OPC and the TIO, should encourage Communications Alliance to develop guidelines for industry participants to conduct PIAs of emerging technologies, applications and services. In Chapter 47, the ALRC recommends that the OPC should develop and publish PIA Guidelines tailored to the needs of organisations.[138]

Recommendation 71–4 The Australian Communications and Media Authority, in consultation with the Office of the Privacy Commissioner, Communications Alliance, the Telecommunications Industry Ombudsman, and other relevant stakeholders, should develop and publish guidance that addresses privacy issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping.

---

136 Optus, *Submission PR 532*, 21 December 2007.
137 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.
138 Rec 47–5.

Telecommunications regulators

71.120 Several bodies are involved in the regulation of the telecommunications industry. ACMA is a statutory authority[139] with specific regulatory powers conferred on it by a number of Acts, including the *Telecommunications Act* and the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth). The TIO is an industry body that investigates and determines complaints by users of carriage services,[140] including complaints about privacy.[141] The OPC deals with complaints of interference with privacy in the telecommunications industry. The various issues raised by the involvement of multiple regulators in the telecommunications industry are considered in more detail in Chapter 73. This chapter considers some of the functions of the OPC and ACMA under the *Telecommunications Act*.

Codes and standards

71.121 Under ss 117 and 134 of the *Telecommunications Act*, the Privacy Commissioner must be consulted about industry codes and standards that deal with privacy issues. In 2006–07, the Privacy Commissioner provided advice in respect of eight codes being developed pursuant to the *Telecommunications Act*.[142] The Privacy Commissioner must also be consulted:

- before ACMA takes certain steps to promote compliance with an industry code relating to a matter dealt with by the NPPs or an approved privacy code;[143] and

- about the way in which law enforcement bodies certify that disclosure of telecommunications information is reasonably necessary for the enforcement of the criminal law.[144]

71.122 Communications Alliance has developed a number of codes under Part 6 of the *Telecommunications Act* which contain privacy provisions or references to relevant privacy legislation.[145] In order to minimise confusion and duplication for the telecommunications sector, Communications Alliance has finalised and published a

---

139 *Australian Communications and Media Authority Act 2005* (Cth) s 8(1).
140 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 128(4).
141 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, cl 4.1.
142 Office of the Victorian Privacy Commissioner, *Annual Report 2006–07* (2007), [1.7.3].
143 *Telecommunications Act 1997* (Cth) ss 121, 122.
144 Ibid s 282(8).
145 See, eg, Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2003); Australian Communications Industry Forum, *Industry Code—Handling of Life Threatening and Unwelcome Calls Industry Code*, ACIF C525 (2006); Australian Communications Industry Forum, *Industry Code—Credit Management*, ACIF C541 (2006); Australian Communications Industry Forum, *Industry Code—Billing Industry Code*, ACIF C542 (2003); Australian Communications Industry Forum, *Industry Code—Priority Assistance for Life Threatening Medical Conditions Industry Code*, ACIF C609 (2007); Australian Communications Industry Forum, *Integrated Public Number Database (IPND) Data Provider, Data User and IPND Manager*, ACIF C555 (2002); Australian Communications Industry Forum, *Industry Code—Complaint Handling Industry Code*, ACIF C547 (2004).

single code that captures the majority of its consumer industry codes, and has submitted it to ACMA.[146]

71.123 The OPC submitted that Part 6 of the *Telecommunications Act* does not define clearly the Privacy Commissioner's powers to comment on whether a code derogates from the *Privacy Act*. In addition, the *Telecommunications Act* does not appear to provide that the Privacy Commissioner must be satisfied with a code before it is registered. The OPC believes that these provisions should be strengthened. For example, s 117 should provide specifically for the Privacy Commissioner to state whether, in his or her opinion, the proposed code 'derogates' materially from the provisions of the *Privacy Act*.

71.124 In DP 72, the ALRC did not propose any major amendments to the code provisions under the *Telecommunications Act*. Part 6 of the *Telecommunications Act* should be considered as part of the recommended review of telecommunications regulation.[147] The ALRC did express the view, however, that the provisions relating to the OPC's role in the development of industry codes and standards should be strengthened. The ALRC therefore proposed that:

- s 117(1)(k) of the *Telecommunications Act* should be amended to provide that ACMA can register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, only if it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied with the code; and

- s 134 of the *Telecommunications Act* should be amended to provide that ACMA can determine, vary or revoke an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, only if it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied with the standard.[148]

Submissions and consultations

71.125 A number of stakeholders supported the proposals.[149] The DBCDE submitted that it is arguable that the proposals only formalise current arrangements and do not extend the Privacy Commissioner's powers.[150] The Department also submitted

---

146 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

147 Rec 71–2.

148 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 63–12, 63–13.

149 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

150 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

however, that primary responsibility for deciding whether to make, vary or revoke a standard should remain with ACMA, and that it is inappropriate for the Privacy Commissioner to have a power of veto over an important aspect of telecommunications administration. [151]

71.126 ACMA submitted that the proposed amendments to ss 117(1)(k) and 134 were unnecessary. It noted, however, that if it is considered appropriate to proceed with the proposals, the amendments should be narrowed to apply only in the circumstances where the Privacy Commissioner is dissatisfied because of a derogation of the requirements of the *Privacy Act*.[152]

71.127 One telecommunications commentator supported the proposals, but submitted that:

- s 117 also should provide specifically for the Privacy Commissioner to state if, in his or her opinion, the proposed code materially 'derogates' from the provisions of the *Privacy Act*; and

- ACMA should not be able to deregister a code that deals with privacy matters unless it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied that deregistering the code will not result in the relevant sector of the telecommunications industry being less adequately regulated in relation to privacy protection requirements than while the Code was in force.[153]

ALRC's view

71.128 The *Telecommunications Act* should provide for a more formal process for ACMA to consult with the OPC when registering codes, or determining or varying industry standards. In the ALRC's view, ACMA should continue to have primary responsibility for the development of codes and industry standards. The ALRC therefore recommends that the Privacy Commissioner's view should be taken into account by ACMA when registering a code, or determining or varying an industry standard; but the Privacy Commissioner should not have a power to veto the registration of a code or the determination or variation of an industry standard.

71.129 ACMA should not be able to revoke an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with the Privacy Commissioner. Consultation on the revocation of codes and industry standards should be included in the memorandum of understanding between the Privacy Commissioner and ACMA recommended in Chapter 73.

---

151 Ibid.
152 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.
153 I Graham, *Submission PR 427*, 9 December 2007.

Recommendation 71–5 Section 117(1)(k) of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority cannot register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

Recommendation 71–6 Section 134 of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority cannot determine or vary an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

Reporting

71.130 Part 13 of the *Telecommunications Act* requires carriers, carriage service providers and number-database operators to create records of certain disclosures of protected information.[154] These records must be provided to ACMA at the end of each financial year.[155] The Privacy Commissioner monitors compliance with the record-keeping requirements under the Act.[156]

71.131 The OPC stated that it understands that only one reason need be recorded for the disclosure and suggested that the ALRC consider whether, where there is more than one applicable reason for the disclosure, it would be appropriate for each reason to be recorded.[157] The OPC also noted that participants in the telecommunications industry are not required to report disclosures of information if the disclosure is: in the performance of a person's duties; to the Australian Security Intelligence Organisation (ASIO); for certain purposes relating to the IPND; by implicit consent of sender and recipient of the communication; or for business needs.[158] The OPC advised that, as part of an enhanced audit and monitoring program over the next few years, the OPC will consider monitoring the record keeping aspects of relevant disclosures.[159]

71.132 In DP 72, the ALRC proposed that s 306 of the *Telecommunications Act* should be amended to provide that each exception upon which a decision to disclose

---

154 *Telecommunications Act 1997* (Cth) s 306. Since the release of DP 72, the *Telecommunications (Interception and Access) Amendment Act 2007* (Cth) amended the *Telecommunications Act 1997* (Cth) so that carriers, carriage service providers and number-database operators are required to create records of certain disclosures under the *Telecommunications (Interception and Access) Act 1979* (Cth): s 306A.

155 *Telecommunications Act 1997* (Cth) s 308.

156 Ibid s 309.

157 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

158 *Telecommunications Act 1997* (Cth) s 306(1)(b).

159 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

information or a document is based is to be recorded when that decision is based on more than one of the exceptions in Divisions 3 or 4 of Part 13 of the Act.[160]

Submissions and consultations

71.133 Optus and the OPC supported the proposal.[161] Optus noted that it already reports single disclosures based on multiple exceptions without inaccurately reporting on the number of disclosures.[162] The Australian Privacy Foundation submitted that it supported the proposal for additional record-keeping, but there also needs to be an express requirement for public reporting of the use of the various exceptions.[163]

71.134 One telecommunications commentator supported the proposal, but submitted that it was unclear under the ALRC's proposals whether the additional information must be reported to ACMA or only recorded by the telecommunications service provider. She also noted that ACMA has been making disclosure statistics publicly available in it's a annual reports for a number of years, but noted that the *Telecommunications Act* does not require ACMA to issue public reports in that regard. She submitted that s 308 should be amended to ensure that future ACMA management cannot decide simply to cease making such information publicly available.[164]

71.135 Telstra objected to the proposal. In Telstra's view, the proposal is unnecessary and only creates additional compliance costs.

> The ALRC proposes that each exception relied upon for a decision to disclose information should be recorded. In reality, however, disclosures are only ever made under a specific exception in Part 13, rather than under a number of exceptions.

71.136 Telstra also submitted that there is no regulatory benefit in recording all possible exceptions under which a disclosure could have been made, when in reality it was made under one particular exception. The rationale for the recording obligation is that the regulator can audit the records and ascertain whether the disclosure practice of the carrier or carriage service provider has been adequate. Telstra submitted that it is difficult to see how an additional record that the disclosure in question could also have been made under another exception would further this regulatory objective.[165]

---

160 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–14.
161 Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
162 Optus, *Submission PR 532*, 21 December 2007.
163 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
164 I Graham, *Submission PR 427*, 9 December 2007.
165 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

71.137 ACMA and the DBCDE questioned whether the benefits of enhanced information relating to disclosure are significant, and suggested that such a proposal would result in an unjustified cost for industry.[166]

ALRC's view

71.138 Telecommunications service providers should report on when they disclose information pursuant to one of the exceptions in Part 13. Each exception upon which a decision to disclose information or a document is based, however, does not need to be recorded when that decision is based on more than one of the exceptions in Part 13 of the Act. The ALRC notes that disclosures are not made under a number of exceptions in Part 13. The ALRC also accepts that there is little regulatory benefit in recording all possible exceptions under which a disclosure could have been made, when in reality the disclosure was made under one particular exception.

71.139 The ALRC does not recommend that the *Telecommunications Act* should be amended to provide that ACMA must include the information reported by telecommunications service providers under s 308 of the Act in its annual report. The ALRC notes that ACMA currently publishes this information in its annual report. The publication of this information is desirable as it promotes transparency and accountability, however, no case for a legislative requirement in this regard has been made out. If ACMA ceases to make this information publicly available, a legislative amendment could be considered.

166 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

72. Exceptions to the Use and Disclosure Offences

Contents

Introduction

72.1 This chapter considers the exceptions to the use and disclosure offences under Part 13 of the *Telecommunications Act 1997* (Cth). The chapter first considers how the exceptions interact with the *Privacy Act 1988* (Cth). The chapter then discusses whether the scope of some of the exceptions under Part 13 should be confined, or aligned with similar exceptions under the *Privacy Act*.

72.2 The next section examines the protection of public number directories. This section considers the regulation of the Integrated Public Number Database (IPND) and public number directories not sourced from the IPND. The final section discusses whether public number directories are desirable and whether telecommunications services providers should be able to charge for unlisted numbers.

Telecommunications Act 1997 (Cth)

72.3 Part 13 of the *Telecommunications Act* regulates the use and disclosure of information obtained by certain bodies during the supply of telecommunications services. It makes it an offence (punishable by up to two years imprisonment) for certain participants in the telecommunications industry (referred to in this chapter as 'telecommunications service providers')—namely, carriers, carriage service providers, telecommunications contractors, and employees of carriers, carriage service providers and telecommunications contractors; eligible number-database operators;[1] and emergency call persons—to use or disclose information or a document relating to the:

- contents of a communication carried, or being carried, by a carrier or carriage service provider;
- carriage services supplied or intended to be supplied by a carrier or carriage service provider; or
- affairs or personal particulars (including any unlisted telephone number or any address) of another person.[2]

72.4 The Act specifies a number of exceptions to these 'primary use/disclosure offences'. These exceptions include that the use or disclosure is: made in the performance of a person's duties as an employee of a carrier, carriage service provider or a telecommunications contractor; required or authorised by or under law; connected with any other carrier or carriage service provider carrying on its business as a carrier or carriage service provider; or consented to by the subject of the information or document.[3]

---

1 *Telecommunications Act 1997* (Cth) s 272. There are currently no eligible number-database operators as no determination is in force under s 472(1).

2 Ibid ss 276–278.

3 Ibid ss 279–294. These exceptions are discussed in detail below.

72.5 The Act also regulates the secondary use and disclosure of protected information.[4] For example, a person to whom information was disclosed because the disclosure was required or authorised by or under law is prohibited from using or disclosing the information, unless the further use and disclosure is also required or authorised by or under law.[5] A person who contravenes the secondary use and disclosure provisions is also guilty of an offence punishable by up to two years imprisonment.[6]

72.6 The *Telecommunications Act* requires telecommunications providers to record and report to the Australian Communications and Media Authority (ACMA) on certain disclosures of information under the Act.[7] In 2006–07, participants in the telecommunications industry made 1,165,391 reported disclosures pursuant to exceptions under Part 13 of the *Telecommunications Act*. This was an increase of 221,024 or 23% over the previous reporting year.[8]

Interaction between the *Privacy Act* and the *Telecommunications Act*

72.7 As discussed in Chapter 71, Part 13 does not refer to 'personal information'. The information protected by Part 13 would, however, include 'personal information' as defined in the *Privacy Act*.

72.8 An organisation that uses or discloses personal information in a way that is authorised under the *Telecommunications Act* will not be in breach of National Privacy Principle 2 (NPP 2). An act or practice engaged in pursuant to any of the exceptions under Part 13 is an act or practice that is 'authorised by or under law' for the purposes of NPP 2.[9] This is confirmed by s 303B of the *Telecommunications Act*, which provides that a use or disclosure permitted under that Act is a use or disclosure that is 'authorised by law' for the purposes of the *Privacy Act*.[10]

72.9 If a telecommunications service provider engages in an act or practice that does not comply with one of the exceptions under Part 13, the act or practice would not be 'authorised by or under law' and so may breach NPP 2. This is supported by s 303C of the *Telecommunications Act*, which provides that a prosecution for an offence relating to the use or disclosure of protected information under the *Telecommunications Act*

4 Ibid ss 296–303A.
5 Ibid s 297.
6 Ibid s 303.
7 Ibid ss 306, 308. The Act does not require uses to be reported.
8 Australian Communications and Media Authority, *Annual Report 2006–07* (2007), App 12. In 2005–06, participants in the telecommunications industry made 944,367 reported disclosures pursuant to exceptions under Part 13 of the *Telecommunications Act*. This was an increase of 58,901 or 6.65% over the previous reporting year: Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145. The *Telecommunications Act* does not require all disclosures to be reported.
9 See Ch 25.
10 *Telecommunications Act 1997* (Cth) s 303B.

does not prevent civil proceedings or administrative action being taken under the *Privacy Act* for the same breach.[11]

72.10 It is unclear, however, whether the exceptions under Part 13 provide the *only* circumstances in which it is lawful to use or disclose information protected under the Part. In particular, it is unclear whether ss 280(1)(b) and 297 of the *Telecommunications Act* would allow a telecommunications service provider to rely on the exceptions under NPP 2 to disclose information in addition to disclosure permitted under Part 13. This issue is discussed further below.

Exceptions to the use and disclosure offences

72.11 The exceptions under Part 13 of the *Telecommunications Act* provide for a range of circumstances in which carriers and carriage service providers may use or disclose information. It has been argued that many of the exceptions are unnecessarily broad and do not provide a sufficient level of protection of personal information in the telecommunications industry.[12] This section of the chapter considers whether the scope of some of the exceptions under Part 13 should be confined, or aligned with similar exceptions under the *Privacy Act*.

Performance of person's duties

72.12 Sections 279 and 296 of the *Telecommunications Act* provide that the primary and secondary use and disclosure of information is permitted if the use or disclosure is made in the performance of that person's duties as an employee[13] or contractor.[14] It has been noted that the exception is necessary for 'the myriad of day-to-day communications between employees about connecting, disconnecting and billing customers'.[15]

72.13 AAPT noted that the exception seems to imply that as long as someone is an employee of a supplier, and is embarking on duties associated with that employment, then they can use and disclose personal information in any way they see fit.

> We are confident that this is not the intended reading of this section, and it is entirely at odds with the *Privacy Act 1988* and its requirements when it comes to the use and disclosure of personal information.

---

11 Ibid s 303C.

12 Electronic Frontiers Australia Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, [30]–[51]. See also AAPT Ltd, *Submission PR 87*, 15 January 2007.

13 An employee of a carrier, carriage service provider, telecommunications contractor, number-database operator, number-database contractor, a person who operates an emergency call service or an emergency call contractor: *Telecommunications Act 1997* (Cth) s 279(1), (3), (5).

14 A telecommunications contractor, number-database contractor or an emergency call contractor: Ibid s 279(2), (4), (6).

15 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 6. An eligible person or an eligible number-database person is not required to report to ACMA the number of disclosures they make under ss 279 and 296: *Telecommunications Act 1997* (Cth) s 306(1).

> The Act also leaves itself open to interpretation about what we consider are key privacy consumer protection mechanisms. This includes not allowing Sales and Marketing people to use the detail of a call to attempt to market to these customers based on these details.[16]

72.14 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC asked whether the exception is too broadly drafted; is resulting in the inappropriate use or disclosure of personal information; and, if so, how the exception should be confined.[17]

72.15 The ALRC outlined two options to confine the exception. The first option was to amend the exception so that it referred to certain duties of an employee or contractor, including connecting and disconnecting telecommunications services and billing. The second option was to bring the exception more closely into line with the 'Use and Disclosure' principle in the model Unified Privacy Principles (UPPs), under which an agency or organisation may use or disclose personal information for a purpose (the secondary purpose) other than the primary purpose of collection if both of the following apply, the:

- secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

- individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.[18]

Submissions and consultations

72.16 The Department of Broadband, Communications and the Digital Economy (DBCDE) submitted that the ALRC should examine whether the exception is resulting in the inappropriate use and disclosure of personal information before recommending that the exception be confined.[19] Some stakeholders submitted that they were unaware of any situations where the exception has resulted in the inappropriate use or disclosure of information.[20]

72.17 Other stakeholders submitted that the exception is too broadly drafted and should be confined.[21] Some submitted that the exception should specify certain duties of an employee or contractor, including connecting and disconnecting

---

16 AAPT Ltd, *Submission PR 87*, 15 January 2007.
17 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–1.
18 See Ch 25.
19 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.
20 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.
21 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

telecommunications services or billing, where 'billing' means billing of the carriage service provider's own customers.[22] Optus and Telstra submitted, however, that it would be impossible to define all the different functions that cover the provision of a carriage service, and that these functions will change over time as products and technologies change.[23]

72.18 The Office of the Privacy Commissioner (OPC) submitted that the exception should be aligned with the 'Use and Disclosure' principle in the model UPPs.[24] One stakeholder submitted, however, that this would not be appropriate in the telecommunications context. She noted that telecommunications service providers do not always 'collect' personal information—for example, some information is automatically generated in the originating carrier's network—and so there will not always be a primary or secondary purpose of collection. She also argued that most individuals would have little knowledge about how telecommunications networks operate so would not know what would be the primary purpose of collection.[25]

72.19 It was also submitted that the exception should be amended to prohibit the disclosure of unlisted number information from the IPND or anywhere else, if the exception is interpreted to allow this; and to specify that the exception only applies 'where it is reasonably necessary for the employee to disclose or use the information or document in order to perform those duties effectively'.[26]

72.20 Other stakeholders strongly opposed any proposal to confine the exception. For example, AAPT submitted that the exception should not be confined, given the range of tasks that are required to deliver a telecommunications service.[27] Telstra submitted that it interprets the exception so it cannot result in an employee using information for a purpose which may be within the scope of his or her employment but is otherwise unlawful.

> Accordingly, in relation to personal information, any use or disclosure by an employee of such information has to comply with the NPPs. There are also other statutory and common law constraints on Telstra (eg confidentiality) which would limit the ability of employees to deal with information … It is therefore unnecessary to further confine the exception.[28]

---

22 I Graham, *Submission PR 427*, 9 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

23 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

24 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. The DBCDE also supported this option, but noted that there may be issues with what was the 'primary purpose of the collection' in the telecommunications context: Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

25 I Graham, *Submission PR 427*, 9 December 2007.

26 Ibid. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. *Telecommunications (Interception and Access) Act 1979* (Cth) s 7 provides a similar exception.

27 AAPT Ltd, *Submission PR 338*, 7 November 2007. See also Optus, *Submission PR 532*, 21 December 2007.

28 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

ALRC's view

72.21 The ALRC does not make any recommendation to confine the scope of the exception under ss 279 and 296 of the *Telecommunications Act*. Stakeholders did not provide any evidence that the exception was resulting in the inappropriate use or disclosure of personal information.

72.22 The ALRC considered confining the scope of the exception to certain duties of an employee or contractor. In the ALRC's view, however, this option would be unworkable in a complex and changing telecommunications environment.

72.23 The ALRC also considered aligning the exception with the recommended 'Use and Disclosure' principle. The ALRC was concerned, however, that confining the scope of the exception in this way could have unforeseen consequences and prevent the provision of telecommunications services. Further, information protected under Part 13 will not always be 'collected'. The proposal would therefore result in the exception relating to only some of the information currently protected under Part 13.

72.24 The ALRC also considered whether the exception should be amended to require that a use or disclosure is 'reasonably necessary' in order for an employee to perform their duties effectively. In the ALRC's view, this is already an implied requirement of the exception.

72.25 The ALRC notes that one stakeholder raised the issue of whether the exception permitted the use and disclosure of unlisted numbers held on the IPND or otherwise. The ALRC did not receive any information that this exception was resulting in the inappropriate disclosure of this information. In the ALRC's view, the use and disclosure of unlisted numbers should be considered in the review of telecommunications legislation recommended in Chapter 71.[29] The use and disclosure of unlisted numbers and other information contained in the IPND is discussed below.

72.26 In Chapter 73, the ALRC recommends that ACMA, in consultation with relevant stakeholders, should develop and publish guidance on telecommunications privacy, including on the exceptions in Part 13. This guidance should provide examples of when a use or disclosure is made in the performance of a person's duties as an employee of a telecommunications service provider.[30]

Required or authorised by or under law

72.27 Sections 280(1)(b) and 297 of the *Telecommunications Act* provide that a primary or secondary use or disclosure of information or document is permitted if the

---

29 Rec 71–2. The ALRC notes that this issue was addressed in Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004). In the ALRC's view, however, the *Telecommunications Act* remains unclear about when unlisted numbers may be disclosed.

30 Rec 73–9.

use or disclosure is required or authorised by or under law. NPP 2, and the 'Use and Disclosure' principle in the model UPPs, provide for a similar exception.[31] ACMA has reported that 21,541 disclosures were made under s 280 in 2006–07,[32] compared to 13,634 in 2005–06.[33]

72.28 It is unclear whether ss 280(1)(b) and 297 would allow a telecommunications service provider to rely on the exceptions under NPP 2 to disclose information (for example, for direct marketing) in addition to those exceptions under Part 13 of the *Telecommunications Act*.[34] While Note 2 to NPP 2 states that the exceptions to NPP 2 do not 'require' an organisation to disclose personal information, it could be argued that the exceptions 'authorise' the use and disclosure of personal information. Some stakeholders argue, however, that the exceptions to NPP 2 are not general authorisations to disclose.[35]

72.29 It is arguable that when Part 13 of the *Telecommunications Act* was enacted Parliament turned its mind to the use and disclosure of information and documents obtained during the supply of telecommunications services, and that it would be contrary to the intention of Parliament to weaken the protection offered by Part 13 to allow the uses and disclosures permitted under NPP 2.

72.30 While s 303B of the *Telecommunications Act* provides that a use or disclosure permitted under that Act is a use or disclosure that is authorised by law for the purposes of the *Privacy Act*,[36] neither the *Privacy Act* nor the *Telecommunications Act* provide that the uses and disclosures permitted under NPP 2 are authorised for the purposes of s 280 of the *Telecommunications Act*.

72.31 Section 303B was introduced by the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states that the provision:

> will make it clear that a disclosure or use of information by a person permitted under Divisions 3 and 4 [of Part 13 of the *Telecommunications Act*] is a disclosure or use authorised by law for the purposes of the *Privacy Act 1988* or an approved privacy code.

---

31 Rule 6.1(c)(f) of the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) provided an identical exception. The scope of the 'required or authorised by or under law' exception in the context of the *Privacy Act 1988* (Cth) is discussed in Ch 16.

32 Australian Communications and Media Authority, *Annual Report 2006–07* (2007), Appendix 12.

33 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145.

34 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

35 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

36 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [427].

72.32 The Explanatory Memorandum does not address whether a use or disclosure permitted by exceptions under NPP 2 is authorised by law for the purposes of Part 13 of the *Telecommunications Act*.[37] One view is that, had the Parliament intended the exceptions under NPP 2 to apply to information or documents protected under Part 13, it would have addressed this issue in the legislation, or at least in the Explanatory Memorandum.

72.33 Further, it is a principle of statutory interpretation that provisions of general application give way to specific provisions when in conflict.

> When the legislature has given its attention to a separate subject and made provisions for it, the presumption is that a subsequent general enactment is not intended to interfere with the special provision unless it manifests that intention very clearly. Each enactment must be construed in that respect according to its own subject matter and its own terms.[38]

72.34 It could be argued that the subsequent enactment of the general provisions of NPP 2 in the *Privacy Act* do not apply in addition to the exception under Part 13 because the Act does not state that intention 'very clearly'.

72.35 In DP 72, the ALRC proposed that ss 280(1)(b) and 297 of the *Telecommunications Act 1997* (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the proposed 'Use and Disclosure' principle under the *Privacy Act*, if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.[39]

Submissions and consultations

72.36 A number of stakeholders supported the proposal.[40] For example, the DBCDE submitted that the proposal has merit on policy grounds—that one Act should not permit what the other is clearly intending to prevent—and would clarify the interaction between the two Acts.[41]

72.37 The Australian Privacy Foundation also supported the proposal but submitted that ss 280(1)(b) and 297 should be amended to permit a use or disclosure if it is required or 'specifically authorised' by or under a law.[42] One stakeholder supported the proposal, and noted that s 280(1)(a) also should be amended to refer to uses or

---

37 The Explanatory Memorandum does, however, outline the exception under s 280 in the section about the relationship with the *Privacy Act*: Ibid, [426].

38 *Barker v Edger* [1898] AC 748, 754; accepted by the High Court of Australia in *Bank Officials' Association (South Australian Branch) v Savings Bank of South Australia* (1923) 32 CLR 276. See D Gifford, *Statutory Interpretation* (1990), 109.

39 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–2.

40 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

41 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

42 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also I Graham, *Submission PR 427*, 9 December 2007.

disclosures that are required or authorised by the *Telecommunications (Interception and Access) Act 1979* (Cth).[43]

72.38 Other stakeholders strongly opposed the proposal. Optus submitted that the outcome of such a proposal would be to prevent the telecommunications industry from using the personal information of its customers for the secondary purpose of direct marketing, as provided for under NPP 2.1.

> This would be a perverse outcome, resulting in an entire industry being barred from using information that is permissible under the *Privacy Act* currently and accessible to all other Australian industries.[44]

72.39 Telstra submitted that the ALRC's interpretation of the exception in DP 72 was incorrect. In Telstra's view, a use or disclosure under the NPPs is clearly a use or disclosure that is authorised by law. Telstra submitted that the *Privacy Act* should not be treated any differently from other legislation which authorises or compels disclosure of information. Telstra submitted that to do otherwise would create significant confusion and major compliance problems for members of the telecommunications industry.[45]

ALRC's view

72.40 Sections 280(1)(b) and 297 of the *Telecommunications Act* should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the 'Use and Disclosure' principle in the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*. The *Privacy Act* should not permit uses and disclosures that the *Telecommunications Act* is clearly intended to prevent. Further, such an amendment would clarify the interaction between the two Acts.

72.41 Rather than confusing telecommunications service providers, such an amendment would clarify that the permitted uses and disclosures of information or documents obtained during the supply of telecommunications services are contained in the *Telecommunications Act*. This is preferable to the current situation where there is confusion about whether the use and disclosure of this information is regulated by two sets of inconsistent exceptions under two Acts.

72.42 The ALRC acknowledges, however, that this is a significant amendment and may not reflect current practice by telecommunications service providers. As noted in Chapter 71, there have been significant developments in the telecommunications industry since the enactment of the *Telecommunications Act*. Telecommunications service providers may need to use and disclose information and documents for purposes that were not anticipated when Part 13 was enacted.

---

43 I Graham, *Submission PR 427*, 9 December 2007.
44 Optus, *Submission PR 532*, 21 December 2007.
45 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

72.43 The ALRC has undertaken an analysis of the exceptions under Part 13 of the *Telecommunications Act* and the *Privacy Act*, and identified that the exceptions under NPP 2 permit the use and disclosure of personal information in circumstances that are not currently permitted under Part 13. It is appropriate that telecommunications service providers can use and disclose information, other than information obtained during the supply of telecommunications services, in accordance with these exceptions.

72.44 The ALRC has concluded, however, that only some of the exceptions under NPP 2 should be available to telecommunications service providers in relation to information obtained during the supply of telecommunications services. These exceptions are discussed below.

72.45 The ALRC considered whether the *Telecommunications Act* should be amended to allow telecommunications service providers to access these exceptions under the *Privacy Act* or whether they should be transferred to the *Telecommunications Act*. The ALRC has concluded that, in the interest of clarity, all the exceptions to the offence provisions in Part 13 should be grouped together in the *Telecommunications Act*.

Recommendation 72–1 Sections 280(1)(b) and 297 of the *Telecommunications Act 1997* (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.

Unlawful activities

72.46 NPP 2.1(f) provides that an organisation may use or disclose personal information about an individual if the organisation has reason to suspect that 'unlawful activity' has been, is being, or may be engaged in, and the use or disclosure is a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities. Suspected unlawful activity would usually relate to the organisation's operations.[46] For example, an organisation might use or disclose personal information under this exception when investigating fraudulent activity of an employee or a customer. No such exception exists in Part 13 of the *Telecommunications Act*.

72.47 The ALRC's recommendation to amend ss 280(1)(b) and 297 of the *Telecommunications Act* would prevent a telecommunications service provider from using or disclosing information or documents obtained during the supply of telecommunications services for the purpose of investigating and reporting on unlawful activities under NPP 2.1(f). Telecommunications service providers would still be able

46 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001).

to use and disclose 'personal information' other than information obtained during the supply of telecommunications services in accordance with NPP 2.1(f).

72.48 Telecommunications service providers are no different from other organisations regulated under the *Privacy Act* in that they need to be able to investigate, and report on,[47] suspected wrongdoing. The ALRC has concluded, therefore, that a telecommunications service provider should be able to use or disclose information or a document regulated by Part 13[48] if it suspects unlawful activity, and the use or disclosure is necessary for the investigation of the matter or in reporting its concerns to relevant persons or authorities.

Recommendation 72–2 The *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure of information or a document is permitted if a person has reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

Direct marketing

72.49 The ALRC's recommendation to amend ss 280(1)(b) and 297 of the *Telecommunications Act* would limit a telecommunications service provider's ability to use information or a document obtained during the supply of telecommunications services for direct marketing.[49]

72.50 The recommendation would not prevent completely the use of information for direct marketing. Telecommunications service providers would be able to use and disclose 'personal information', other than information or a document obtained during the supply of telecommunications services, for direct marketing on the same basis as under the 'Direct Marketing' principle in the model UPPs.[50] For example, a telecommunications service provider could purchase a customer list for the purpose of direct marketing. The use and disclosure of this information would be regulated under the *Privacy Act*.

---

47 Employees of telecommunications service providers are permitted to disclose this information voluntarily to intelligence and enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (Cth). See discussion in Ch 73.

48 This includes information or documents relating to the content or substance of communications, not the actual content or substance of a communication. The content and substance of communications is regulated under the *Telecommunications (Interception and Access) Act*.

49 Rec 72–1.

50 See Ch 26.

72.51 Further, s 289(1)(b)(ii) of the *Telecommunications Act* would allow a telecommunications service provider to use and disclose the affairs or personal particulars of a person for the purpose of direct marketing if the person consented to the information being used or disclosed for that purpose.[51]

72.52 The telecommunications industry has undergone significant changes since the enactment of Part 13, including the privatisation of Telstra, business diversification, specialisation and the entry of new niche industry participants.[52] The ALRC acknowledges that in this increasingly competitive industry, telecommunications service providers need to use and disclose personal information for the purpose of direct marketing.

72.53 In Chapter 26, the ALRC recommends a 'Direct Marketing' principle (UPP 6). UPP 6.1 provides that an organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing in certain circumstances—that is, where the:

- individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and

- organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.

72.54 The ALRC has concluded that, subject to one limitation, a telecommunications service provider should be able to use and disclose an existing customer's 'personal information', including information obtained during the supply of telecommunications services, for the purpose of direct marketing on the same basis as recommended under the 'Direct Marketing' principle. The limitation is that the following information should not be used for the purpose of direct marketing without an existing customer's consent:

- information or a document relating to the contents of a communication carried, or being carried, by a carrier or carriage service provider; and

- information or a document relating to the carriage services supplied or intended to be supplied by a carrier or carriage service provider.

72.55 As noted in Chapter 71, this information would include the telephone numbers of the parties involved, the time of a call and its duration, the Internet Protocol (IP) address used for a session, and the start and finish time of each session. The ALRC is

---

51 See discussion of *Telecommunications Act 1997* (Cth) s 289(1)(b)(ii) below.

52 These developments are discussed in Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 22.

concerned that a telecommunications service provider could use this information to monitor when, how and with whom an individual communicates, and what websites they access, for the purpose of sending direct marketing communications to that individual. This information only should be used or disclosed for the purpose of direct marketing with the consent of the individual.[53] For example, existing customers of a telecommunications service provider may want to receive direct marketing communications based on information relating to their use of a telecommunication service.

Recommendation 72–3 The *Telecommunications Act 1997* (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the *Privacy Act* about an individual who is an existing customer aged 15 or over for the purpose of direct marketing only where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing;

(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(c) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider.

72.56 Under UPP 6.2 an organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing in a number of circumstances.

72.57 A telecommunications service provider should not be able to use information obtained during the supply of a telecommunications services about an individual who is not an existing customer. Information relating to the parties to a communication will often pass over a number of telecommunications service providers' networks. It is inappropriate in these circumstances for a telecommunications service provider to use information relating to an individual who is not an existing customer for the purpose of direct marketing. In the interest of consistency with the 'Direct Marketing' principle, a telecommunications service provider, however, should be able to use and disclose the

53 As noted above, s 289(1)(b)(ii) of the *Telecommunications Act* would allow a telecommunications service provider to use and disclose information for the purpose of direct marketing with consent.

personal information of an existing customer who is under 15 years in accordance with UPP 6.2.

Recommendation 72–4 The *Telecommunications Act 1997* (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the *Privacy Act* about an individual who is an existing customer and is under 15 years of age for the purpose of direct marketing only in the following circumstances:

(a) either the:

(i) individual has consented; or

(ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and

(b) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider;

(c) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;

(d) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(e) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.

72.58 UPP 6.3 provides that in the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must comply with this requirement within a reasonable period of time and not charge the individual for giving effect to the request. This requirement also should apply in the telecommunications context.[54]

54 See discussion of this requirement in Ch 26.

Recommendation 72–5 The *Telecommunications Act 1997* (Cth) should be amended to provide that in the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:

(a) comply with this requirement within a reasonable period of time; and

(b) not charge the individual for giving effect to the request.

Health information

72.59 The ALRC's recommendation to amend ss 280(1)(b) and 297 of the *Telecommunications Act* also would exclude telecommunications service providers from using information obtained during the supply of telecommunications services for the purpose of health research as permitted under NPP 2.1(d). This exception relates to the use and disclosure of health information where it is necessary for research, or the compilation or analysis of statistics relevant to public health or public safety. Telecommunications service providers do not conduct research or compile or analyse statistics relevant to public health or public safety. In the ALRC's view, this exception is unnecessary in the context of the provision of telecommunications services.

72.60 The ALRC acknowledges, however, that telecommunications service providers collect health information. For example, some telecommunications service providers collect health information for the provision of services to priority assistance customers. The collection of this information would be regulated under the *Privacy Act.* The use and disclosure of this information for the provision of services to priority assistance customers would not be permitted, however, under NPP 2.1(d). It may be permitted under a number of other exceptions under Part 13, including the exception under s 287, relating to a threat to person's life or health, and s 289, where an individual has consented to that use or disclosure or would reasonably expect that use or disclosure.

Law enforcement

72.61 The ALRC's recommendation to amend ss 280(1)(b) and 297 of the *Telecommunications Act* would prevent telecommunications service providers from disclosing personal information obtained during the supply of a telecommunications service to an 'enforcement body', as provided for by NPP 2.1(h) and the 'Use and Disclosure' principle in the model UPPs.

72.62 For the reasons discussed in detail below, this is appropriate. Information obtained during the supply of a telecommunications service should be subject to more stringent rules than those provided for in NPP 2.1(h) and the 'Use and Disclosure' principle in the model UPPs. The ALRC is concerned that information obtained during the supply of telecommunications services could allow law enforcement bodies to monitor and track an individual based on when, how and with whom that individual

communicates; the websites they access; and the location of their mobile phone. Further, the Australian Government has amended the *Telecommunications (Interception and Access) Act* to deal with the disclosure of this information for law enforcement purposes.[55]

72.63 NPP 2.1(h) permits the use or disclosure of personal information for a number of law enforcement purposes by or on behalf of an enforcement body. These purposes include the prevention, detection, investigation or punishment of criminal offences; the enforcement of laws relating to the confiscation of the proceeds of crime; and the protection of the public revenue.

72.64 Most of the uses and disclosures permitted under NPP 2.1(h) would be permitted under the *Telecommunications (Interception and Access) Amendment Act*.[56] For example, s 177 of the *Telecommunications (Interception and Access) Amendment Act* provides that a telecommunications service provider may disclose voluntarily information or a document obtained during the supply of telecommunications services to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or the protection of public revenue.[57]

72.65 It is questionable, however, whether the *Telecommunications (Interception and Access) Amendment Act* would permit a disclosure for the purpose of the prevention, detection, investigation or remedying of 'seriously improper conduct', as provided for under NPP 2.1(h)(iv) and the 'Use and Disclosure' principle in the model UPPs.[58] The prevention, detection, investigation or remedying of 'seriously improper conduct' generally refers to:

> serious breaches of professional standards of conduct regarding the exercise of duties, powers, authorities or responsibilities and which warrant enforcement action by a professional association or other body, eg bringing a profession into disrepute, sexual relations with a patient, corruption and perverting the course of justice.[59]

72.66 This exception is not appropriate in the context of information obtained during the supply of a telecommunications service. The ALRC is concerned that NPP 2.1(h)(iv) is too broad, and would permit disclosure of information to a range of bodies, such as professional associations, that are not subject to the same use and disclosure, retention, and destruction and reporting requirements as enforcement agencies under the *Telecommunications (Interception and Access) Act*.

---

55 As noted in Ch 73, the *Telecommunications (Interception and Access) Amendment Act 2007* (Cth) deleted the law enforcement and protection of public revenue provisions from the *Telecommunications Act* and introduced a new Chapter 4 into the *Telecommunications (Interception and Access) Act 1979* (Cth). Ch 73 discusses these provisions in detail.

56 The definition of 'enforcement body' under the *Privacy Act* and the definition of 'enforcement agency' under the *Telecommunications (Interception and Access) Amendment Act* are broadly similar.

57 This provision is discussed in Ch 73.

58 See Ch 25.

59 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2–1695].

72.67 NPP 2.1(h)(v) permits disclosure of personal information for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal. Section 280 of the *Telecommunications Act* would permit the use and disclosure of information obtained during the supply of a telecommunications service for the implementation of an order of a court or tribunal.[60]

72.68 It is unlikely, however, that the *Telecommunications (Interception and Access) Act* would permit the disclosure of information obtained during the supply of a telecommunications service for proceedings, or a court or tribunal orders, when those proceedings or orders do not relate to the criminal law or a law imposing a pecuniary penalty or the protection of public revenue. This is appropriate in the context of information obtained during the supply of telecommunications service. As outlined in Chapter 71, this information is highly sensitive and should be subject to more stringent protection than that provided under the *Privacy Act*.

72.69 Individuals and telecommunications service providers may not be aware that the *Telecommunications (Interception and Access) Act* provides for the use and disclosure of 'telecommunications data' in a range of circumstances not covered by Part 13. These uses and disclosures would be 'authorised' for the purposes of s 280 of the *Telecommunications Act*. In the interest of clarity, a note should be inserted after s 280 of the *Telecommunications Act 1997* (Cth), cross-referencing to Chapter 4 (Access to telecommunications data) of the *Telecommunications (Interception and Access) Act*.

Recommendation 72–6 A note should be inserted after s 280 of the *Telecommunications Act 1997* (Cth) cross-referencing to Chapter 4 (Access to telecommunications data) of the *Telecommunications (Interception and Access) Act 1979* (Cth).

Threat to person's life or health

72.70 Sections 287 and 300 of the *Telecommunications Act* provide that a primary or secondary use or disclosure of information is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person, and the first person believes on reasonable grounds that the use or disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person. Unlike NPP 2, the provisions do not permit use or disclosure where it is necessary to lessen or prevent a serious threat to 'public health or public safety'. ACMA has reported that 3,980 disclosures were made under this exception in 2006–07,[61] compared to 4,085 disclosures in 2005–06.[62]

---

60 See Ch 16.

61 Australian Communications and Media Authority, *Annual Report 2006–07* (2007), App 12.

62 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145. In 2004–05, there were 885,466 disclosures—an increase of 26% from the previous financial year:

72.71 The guidance notes to the deregistered Australian Communications Industry Forum (ACIF) *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* stated that this provision is aimed at emergency situations.

> A threat to life or health would be interpreted to include threats to safety—bush fires, industrial accidents etc. Health would include mental as well as physical health, although appeals to the threat of stress or anxiety would not generally be sufficient. The rules require the threat is serious and imminent.[63]

72.72 In DP 72, the ALRC proposed that ss 287 and 300 of the *Telecommunications Act* should be amended to provide that a use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to: a person's life, health or safety; or public health or public safety.[64]

Submissions and consultations

72.73 A number of stakeholders supported the proposal.[65] The Australian Privacy Foundation submitted that it supported the proposal provided that the provision retains the 'imminent' qualifier. The Foundation submitted that, without this qualifier, the part of the exception relating to 'public health or safety' could be abused too readily.[66]

72.74 The DBCDE supported the proposal. The Department noted, however, that the proposal to extend the exception to 'public health and safety' could raise issues in relation to the use and disclosure of IPND information for the dissemination of mass outbound warning messages to the population, including on a commercial basis. The DBCDE noted that it had been working closely with Emergency Management Australia to determine if there is a case for a national telephone-based warning system and examining the feasibility of access to the IPND for this purpose. The Department also noted that the proposal did not limit the kinds of organisations to whom the IPND Manager could disclose information. It submitted that the proposal could increase the

---

Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 186.

63 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), 23. Rules 6.1(d) and 7.1(c) of the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) provided for a similar exception.

64 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–3.

65 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

66 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also I Graham, *Submission PR 427*, 9 December 2007.

range of organisations outside the telecommunications industry accessing IPND information.[67]

72.75 A number of stakeholders did not support the proposal. The OPC submitted that the proposal diminishes privacy protection.[68] The OPC also noted that there are a number of exceptions in Part 13 which facilitate the use and disclosure of personal information in an emergency where the threat may be serious but not imminent, for example, s 289.[69]

ALRC's view

72.76 In Chapter 25, the ALRC considers a similar exception under the 'Use and Disclosure' principle. In that chapter the ALRC expresses the view that the requirement that a threat be 'imminent' as well as 'serious' is inappropriate. In the ALRC's view, any analysis of whether a threat is 'serious' must involve consideration of the gravity of the potential outcome as well as the relative likelihood. The ALRC therefore recommends amending the exception to provide that it applies where the relevant threat is serious, but not necessarily imminent.

72.77 Similar wording should be used in the exception under Part 13. This would allow telecommunications service providers to take preventative action to stop a threat from developing to a point where the danger, which one is seeking to avoid, is likely to eventuate. At this point it is often too late to take meaningful preventative action. Further, this formulation strikes an appropriate balance between respecting the privacy rights of an individual and the public interest in averting serious threats to a person's life, health or safety.

72.78 The ALRC does not recommend that ss 287 and 300 should relate to 'public health and safety'. The ALRC notes the concerns expressed by the DBCDE that such an amendment may permit access to IPND information for the purpose of providing services that enable the dissemination of mass outbound warning messages to the public. Later in this chapter, the ALRC concludes that it is unclear when a telecommunications services provider may use or disclose information held on the IPND. In the ALRC's view, the Australian Government should consider extending ss 287 and 300 to apply to 'public health and safety' only when permitted uses or disclosures of information held on the IPND are clarified.

---

67 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

68 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also Optus, *Submission PR 532*, 21 December 2007.

69 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also Optus, *Submission PR 532*, 21 December 2007.

Recommendation 72–7 Sections 287 and 300 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if:

(a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to a person's life, health or safety.

Knowledge of person concerned

72.79 Section 289(1)(b)(i) of the *Telecommunications Act* provides that the use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person, and the other person is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned.

72.80 NPP 2.1(a) contains a similar exception where an individual would reasonably expect an organisation to use or disclose the information for a purpose (the secondary purpose) other than the primary purpose of collection.[70] NPP 2, however, contains the added protection that the secondary purpose must be related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection.

72.81 One stakeholder has noted that s 289(1)(b)(i) and NPP 2.1(a) offer very different levels of protection, and submitted that either the *Privacy Act* or *Telecommunications Act* should be amended to require businesses in the telecommunications sector to comply with NPP 2.1(a) in relation to use and disclosure for secondary purposes. It also noted that the existing protection under s 289(1)(b)(i) in relation to use and disclosure for the primary purpose should not be removed or made any weaker.[71]

72.82 In DP 72, the ALRC proposed that s 289(1)(b)(i) of the *Telecommunications Act* should be amended to provide that a use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person;

---

70 According to the OPC, this means that 'the secondary purpose must be something that arises in the context of the primary purpose': Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

71 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007. See also Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

and the other person has consented to the use or disclosure; or if the use or disclosure is for a purpose other than the primary purpose for which the information was collected (the secondary purpose):

- the secondary purpose is related to the primary purpose and, if the information or document is sensitive information (within the meaning of the *Privacy Act*), the secondary purpose is directly related to the primary purpose of collection; and

- the other person would reasonably expect the person to use or disclose the information.[72]

Submissions and consultations

72.83 A number of stakeholders supported the proposal.[73] The Australian Federal Police, however, submitted that the proposal unnecessarily narrows the exception.[74] The Australian Privacy Foundation submitted that the second limb of the proposal is too broad. The Foundation noted that what is a 'reasonable expectation' in the telecommunications context is difficult to determine. It submitted that privacy protection should rest on a presumption that only uses and disclosures 'necessary' for the provision of a telecommunications service are permitted without consent, unless one of the other exceptions apply.[75]

72.84 One stakeholder questioned the relevance of 'collection' in a telecommunications context; and the feasibility of a 'secondary purpose' test, noting that most individuals have little knowledge about how telecommunication networks operate so they would not be able to know what was a primary purpose of collection.[76]

72.85 The stakeholder also noted that the proposal would require telecommunications service providers to obtain consent for the use and disclosure of information for the primary purpose of collection, and questioned whether this was the ALRC's intent. She also submitted that the proposal would be a significant improvement on the existing exception if the intent was that:

- a use or disclosure for a primary purpose required either consent or that the other person would reasonably expect the person to use or disclose the information; and

---

72 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–4.

73 Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Optus, *Submission PR 532,* 21 December 2007; Australian Communications and Media Authority, *Submission PR 522,* 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512,* 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.

74 Australian Federal Police, *Submission PR 545,* 24 December 2007.

75 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

76 I Graham, *Submission PR 427,* 9 December 2007.

- a use or disclosure for a related secondary purpose required either consent or the same requirements as existing NPP 2.1(a).[77]

72.86 The stakeholder doubted, however, whether such a proposal would provide an appropriate level of protection for all types of information, including mobile phone location information and unlisted and other blocked calling numbers. She submitted that Part 13 should be amended to insert new provisions specifying the circumstances and conditions under which a new category of 'specially protected information' (for example, mobile phone location information, calling number information) may be used or disclosed. She submitted that the exception under s 289(1)(b)(i) should state that it does not apply to 'specially protected information'.[78]

72.87 She also noted that regulators have issued conflicting advice on whether the exception under s 289(1)(b)(i) may be relied on when other exceptions do not apply—such as s 291, which relates to the business needs of other carriers or carriage service providers. In her view, s 291 alone permits the use and disclosure of information to other carriers and carriage service providers. She submitted that s 289(1)(b)(i) should state that it does not apply to disclosures made to a carrier or a carriage service provider (unless consent to the particular disclosure has been obtained).[79]

ALRC's view

72.88 In Chapter 25, the ALRC considers various reformulations of the 'reasonable expectation' exception, but suggests that the current exception under NPP 2 provides the appropriate level of protection for an individual's personal information. The term 'reasonable expectation' imports an objective test of what a hypothetical reasonable individual would expect in the relevant circumstances. This condition is an important, but not particularly onerous, protection against the misuse of an individual's personal information.

72.89 An individual is more likely reasonably to expect the use or disclosure of their information or a document if the use or disclosure is related, or in the case of 'sensitive information' directly related, to the primary purpose for which the information or document came to a telecommunications service provider's knowledge or into its possession.[80] This requirement is appropriate in the telecommunications context.

72.90 Part 13 does not refer to 'sensitive information', but would regulate the use and disclosure of 'sensitive information' as defined under the *Privacy Act*. Section 289(1)(b)(i) has the potential to permit the use and disclosure of information in a broad range of circumstances. The exception under s 289(1)(b)(i) should be confined, therefore, by aligning it with the level of protection afforded to such information under

---

77 Ibid.
78 Ibid.
79 Ibid. *Telecommunications Act 1997* (Cth) s 291 is discussed below.
80 *Telecommunications Act 1997* (Cth) pt 13 protects information and documents that come to a 'person's knowledge' or into a person's 'possession'. See, eg, *Telecommunications Act 1997* (Cth) s 276(1)(b).

the *Privacy Act*. This will ensure that 'sensitive information' obtained during the supply of a telecommunications service receives the same level of protection it would have under the *Privacy Act*.

72.91 The exception under s 289(1)(b)(i) operates to allow the use and disclosure of information that otherwise may not be permitted under other exceptions. This exception, however, should not be given a broad interpretation. To be related, the secondary purpose must be something that arises in the context of the primary purpose for which the information or document came to a telecommunications service provider's knowledge or into its possession. If the information is sensitive information the use or disclosure must be directly related to the primary purpose. This means that there must be a stronger connection between the use or disclosure and the primary purpose for which the information or document came to the person's knowledge or into the person's possession. Further, the test for what an individual would 'reasonably expect' would be applied from the point of view of what an individual with no special knowledge of the telecommunications industry or activity involved would expect.[81]

72.92 While there may be merit in the amendment of s 289 to provide that it does not apply to information such as unlisted numbers and other calling number information, and location information, the ALRC received only one submission on this issue. This issue should be considered as part of the review of the *Telecommunications Act* recommended in Chapter 71. This issue of unlisted numbers and calling number information is discussed below.

72.93 In Chapter 73, the ALRC recommends that ACMA, in consultation with relevant stakeholders, should develop and publish guidance relating to the exceptions under Part 13 of the *Telecommunications Act*. This guidance should set out examples of when s 289(i)(b)(i) may be relied on.

Recommendation 72–8 Section 289 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(a) the other person has consented to the use or disclosure; or

(b) the use or disclosure is made for the purpose for which the information or document came to the person's knowledge or into the person's possession (the primary purpose); or

81 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 35–36.

(c) the use or disclosure is for a purpose other than the primary purpose (the secondary purpose); and

(i) the secondary purpose is related to the primary purpose, and if the information or document is sensitive information (within the meaning of the *Privacy Act*), the secondary purpose is directly related to the primary purpose; and

(ii) the other person would reasonably expect the person to use or disclose the information.

Consent

72.94 Section 289(1)(b)(ii) provides that the use or disclosure by a person of information is permitted if the information relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person and the other person has consented to the use or disclosure. Consent is also an exception under NPP 2.1(b) and the 'Use and Disclosure' principle in the model UPPs.[82]

72.95 The *Telecommunications Act* does not provide a definition of 'consent' for the purposes of s 289 or other provisions.[83] The term 'consent' is defined in the *Privacy Act* to mean 'express consent or implied consent',[84] but remains otherwise undefined. In DP 72, the ALRC proposed that Part 13 of the *Telecommunications Act* should be amended to provide that 'consent' means 'express consent or implied consent'.[85]

Submissions and consultations

72.96 A number of stakeholders supported the proposal.[86] The DBCDE submitted that the proposal has merit, as it would make Part 13 of the *Telecommunications Act* consistent with the *Privacy Act*, *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2007* (Cth).[87]

72.97 Some stakeholders submitted that there should only be a very limited role for 'implied consent' in the telecommunications context. In their view, there are a range of

---

82 See also Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), rr 6.1(b), 7.1(b).

83 See discussion of s 290 below.

84 *Privacy Act 1988* (Cth) s 6(1).

85 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–5.

86 Optus, *Submission PR 532*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

87 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007. The ALRC's recommendation for guidance on 'consent' is discussed further in Ch 73.

uses and disclosures of telecommunications information which should require express consent, such as the disclosure of unlisted numbers and mobile phone location information. It was submitted that this should be provided for in the legislation, and not left to guidance.[88]

ALRC's view

72.98 In the interest of clarity, and consistency with the *Privacy Act*, Part 13 of the *Telecommunications Act* should be amended to provide that 'consent' means 'express consent or implied consent'.

72.99 The specific requirements of consent—particularly as regards the requisite level of voluntariness—are highly dependent on the context in which the personal information is collected, used or disclosed. In other words, what may be required to obtain valid consent in one situation may differ, sometimes significantly, from what is required to obtain consent in another situation. For example, only 'implied consent' may be required when a telecommunications service provider needs to disclose information relating to a customer in order to provide a telecommunications service requested by the customer. 'Express consent', however, may be required when using or disclosing sensitive information, such as an unlisted number.

72.100 In Chapter 73, the ALRC recommends that ACMA, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry. This guidance should explain how consent may be obtained in certain contexts—such as, when an individual is entering an agreement for the provision of services with a telecommunications provider. This guidance should also include advice on when it is appropriate to use the mechanism of bundled consent.

Recommendation 72–9 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that 'consent' means 'express or implied consent'.

Implicit consent

72.101 Section 290 of the *Telecommunications Act* provides that the use or disclosure by a person of information is permitted if the information relates to the contents of a communication made by another person, and having regard to all the relevant circumstances, it might reasonably be expected that the sender and the recipient of the communication would have consented if they had been aware of the use or disclosure. The Explanatory Memorandum to the Telecommunications Bill 1996 (Cth) states that this exception is intended to allow disclosure of public communications, for example,

88 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also I Graham, *Submission PR 427*, 9 December 2007.

where a carrier discusses the content of an online bulletin board, or the content of a pay-television program carried on a cable network.[89]

72.102 In DP 72, the ALRC noted that stakeholders had expressed concerns that this exception may lower the threshold of privacy protection in the telecommunications sector;[90] and that the scope of the exception is unclear and does not protect adequately personal information of third parties referred to in a communication.[91] The ALRC expressed the preliminary view that the provision should be amended to clarify that it relates only to public communications. The ALRC noted, however, that it was interested in stakeholder's views on how the provision could be clarified.[92]

Submissions and consultations

72.103 A number of stakeholders supported the ALRC's preliminary view that s 290 should be amended to clarify that it relates only to public communications.[93] The Australian Privacy Foundation supported this view, but noted that, in the absence of detailed statistics about the use of this exception, it is impossible to tell if it is being abused. The Foundation submitted that there should be a requirement for public reporting of the use of the exception.[94]

72.104 Other stakeholders submitted that the exception was not resulting in inappropriate disclosures and was necessary. For example, Optus submitted that s 290 is necessary to allow a telecommunications service provider passing a call to another carriage service provider to allow a call to be terminated. For example, information will need to be passed to another network to permit the termination of a call that originates on the Optus network and terminates on a Vodafone mobile network or an international carrier network.[95]

72.105 Telstra submitted that this exception is required so that the 'forwarding' of emails and short message services (SMS), which may result in a disclosure of personal information of the original sender, is not prohibited. Telstra noted that, while there is an argument that it is the forwarder of the message who discloses the information and not the telecommunications service provider, s 290 puts it beyond doubt that

---

89 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 10. See also Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), 21.

90 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

91 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

92 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–3.

93 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

94 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also I Graham, *Submission PR 427*, 9 December 2007.

95 Optus, *Submission PR 532*, 21 December 2007.

telecommunications service providers have no liability for providing these types of services.[96]

ALRC's view

72.106 The intent of s 290, as expressed in the Explanatory Memorandum to the Telecommunications Bill 1996, is not reflected clearly in the wording of the section. The ALRC is concerned that this lack of clarity may lower the threshold of privacy protection in the telecommunications sector, and does not protect adequately personal information of third parties referred to in a communication. The provision should be amended to clarify that it relates only to public communications.

72.107 Stakeholders argued that this exception is required in its current form for a range of activities that do not relate to public communications. The ALRC has concluded, however, that an amendment to clarify that s 290 relates only to public communications would not prevent these activities, as they are permitted under other exceptions under Part 13 of the *Telecommunications Act*.

72.108 For example, the need to terminate calls that originate on one network and terminate on another would be permitted under s 291 of the *Telecommunications Act*. Telecommunications service providers would not have to rely on s 290 to use and disclose information to diagnose or rectify service problems, as this is clearly permitted under ss 279, 289 and 296 of the *Telecommunications Act*. Further, the access of communications for the purposes of maintenance of a telecommunications system is provided for under the *Telecommunications (Interception and Access) Act*.[97]

72.109 The ALRC acknowledges stakeholder concerns that a telecommunications service provider could be held liable under the *Telecommunications Act* for forwarded emails and SMS which may result in the disclosure of personal information of the original sender.

72.110 Part 13 of the *Telecommunications Act* protects information and documents that come to a telecommunications service provider's knowledge or possession.[98] While a forwarded email or SMS will rarely come to the knowledge of a telecommunications service provider, the communication may come into a telecommunications service provider's possession. Further, the exception under s 290 would not apply where it could not reasonably be expected that the original sender would have consented to the forwarding of an SMS or email. It is therefore arguable that a telecommunications service provider could be held liable under the *Telecommunications Act* for forwarded emails and SMS which may result in the disclosure of personal information of the original sender.

---

96 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

97 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 7 and 108.

98 See, eg, *Telecommunications Act 1997* (Cth) s 276(1)(b).

72.111 It is highly unlikely, however, that a telecommunications service provider would be held liable under the *Telecommunications Act* for this disclosure. It is the forwarder of this information that discloses the information, not the telecommunications service provider. It could also be argued that Part 13 implies that a telecommunications service provider would not breach the offence provisions merely by providing a telecommunications service that enabled the email or SMS to be forwarded. To interpret Part 13 otherwise would require a telecommunications service provider to monitor communications to ensure that they would not result in the unlawful disclosure of information or a document. This result would be both inappropriate and impractical.

72.112 Further, it will be impossible for a telecommunications service provider to ensure that the carriage of every communication that passes over its network does not breach Part 13 of the *Telecommunications Act* or the *Privacy Act*. Telecommunications service providers do not have knowledge or control of every communication that passes over a telecommunications network.

72.113 A number of federal, state and territory laws address this issue. For example, s 112 of *Copyright Act 1968* (Cth) provides that:

> A person (including a carrier or carriage service provider) who provides facilities for making, or facilitating the making of, a communication is not taken to have authorised any infringement of copyright in an audio-visual item merely because another person uses the facilities so provided to do something the right to do which is included in the copyright.

72.114 The *Spam Act* provides that a person must not send certain commercial electronic messages.[99] Section 9 of the *Spam Act* provides that for the purposes of the Act, a person does not 'send' an electronic message, or cause an electronic message to be sent, merely because the person supplies a carriage service that enables the message to be sent.

72.115 Section 32 of the *Defamation Act 2005* (NSW) provides it is a defence to the publication of defamatory matter if:

- the defendant published the matter merely in the capacity, or as an employee or agent, of a 'subordinate distributor' (a 'subordinate distributor' includes an operator of, or a provider of access to, a communications system by means of which the matter is transmitted, or made available, by another person over whom the operator or provider has no effective control);

- the defendant neither knew, nor ought reasonably to have known, that the matter was defamatory; and

---

99 *Spam Act 2003* (Cth) s 16. The *Spam Act* is discussed in Ch 73.

- the defendant's lack of knowledge was not due to any negligence on the part of the defendant.

72.116 As noted above, it is highly unlikely that a telecommunications service provider would be held liable under the *Telecommunications Act* for forwarded emails and SMS which may result in the disclosure of personal information of the original sender. In the interest of certainty, however, the ALRC sees merit in amending Part 13 of the *Telecommunications Act* to provide that a telecommunications service provider is not liable for certain uses and disclosures merely because the provider supplies a service that enables the information to be sent.

72.117 For example, the *Telecommunications Act* could be amended to provide that a telecommunications service provider is not liable under Part 13 of the *Telecommunications Act* if:

- the provider disclosed information or a document merely because the provider supplies a service that enabled the information or document to be sent;

- the provider neither knew, nor ought reasonably to have known, that the disclosure of the information or document would have resulted in a breach of Part 13 of the *Telecommunications Act*; and

- the provider's lack of knowledge was not due to any negligence on the part of the provider.

72.118 This amendment could be considered as a consequential amendment if the ALRC's recommendation to amend s 290 to clarify that the section relates only to public communications is implemented.

Business needs of other carriers or service providers

72.119 Sections 291 and 302 of the *Telecommunications Act* provide that the primary and secondary use or disclosure by a person of information is permitted if: it is made by or on behalf of a carrier or carriage service provider for the purposes of facilitating another carrier or service provider providing a service to the person who is the subject of the information or document; and that person has been or is a customer of the disclosing carrier or carriage service provider, or the other carrier or service provider.

72.120 The provision also contains rules that allow the use or disclosure of information or a document about customers for a purpose connected with a carriage service intermediary arranging the supply of a carriage service by a carriage service provider to a third person.[100]

---

100 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 10–11.

72.121 This provision is designed to allow a use and disclosure that is 'triggered' by some action or request by a customer such as dialling an access code to make use of another carrier. It does not provide for uses and disclosures of subscriber information for activities such as marketing by other carriers or service providers.[101]

72.122 In DP 72, the ALRC noted that stakeholders had raised a number of concerns relating to this exception.[102] These concerns related to the scope of the exception and whether it permitted the use and disclosure of silent numbers, calling number display or location-based information.[103] Concerns were also raised in submissions that telecommunications providers have interpreted s 291 and other provisions under Part 13 to allow the use or disclosure of credit reporting information and credit worthiness information.[104]

72.123 The ALRC expressed the preliminary view that the scope of ss 291 and 302 should be clarified. The ALRC asked whether s 291 and s 302 are resulting in the inappropriate use or disclosure of personal information; and if so, how the exception should be confined. The ALRC also asked whether the exception should be amended to provide that silent and other blocked calling numbers can be used or disclosed only with a person's consent.[105]

72.124 The ALRC outlined two options for reform. The first would be to amend ss 291 and 302 to confine the exception to certain duties of an employee or contractor, including connecting and disconnecting telecommunications services; and limit expressly the circumstances when silent and other blocked calling numbers could be used or disclosed. A second option would be to subject the exception to a requirement that a use and disclosure by a person made for the purpose of performing that person's duties must be related to the primary purpose of collection.

Submissions and consultations

72.125 Some stakeholders submitted that the exception is being abused, and should be confined.[106] The Australian Privacy Foundation submitted that the exception should be amended to require free and informed consent, unless a use or disclosure actually is necessary for the particular service being provided.[107]

---

101 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), 20–21.

102 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [63.81]–[63.94].

103 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

104 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. This issue is discussed later in this chapter.

105 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–4.

106 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; I Graham, *Submission PR 427*, 9 December 2007.

107 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

72.126 One stakeholder submitted that ss 291 and 302 should be amended to: confine the exception to certain duties of an employee or contractor where it is not practical to obtain consent; minimise the need for amendments when new privacy-invasive technologies are developed; and provide that a secondary use or disclosure is permitted only when it is for the same purpose for which the original telecommunications service provider disclosed the information.[108]

72.127 The OPC supported confining the exceptions to: the duties of an employee or contractor, including connecting and disconnecting telecommunications services; prohibiting the use or disclosure of credit reports or credit worthiness information; and requiring that silent and blocked telephone numbers can be used or disclosed only with the consent of the individual.[109]

72.128 Telstra and Optus submitted that the exception under ss 291 and 302 has not resulted in the inappropriate use and disclosure of information.[110] These stakeholders emphasised that the exception is critical to the efficient and effective running of telecommunications in Australia.[111]

72.129 Optus noted that the telecommunications industry relies upon a large number of inter-carrier transfer processes, for example, when a customer wishes to change their mobile provider but wants to keep their mobile number. Optus submitted that, without ss 291 and 302, this process would be undermined. It also submitted that any limitation on the exception under ss 291 and 302 could be used by competitors as a reason to prevent necessary inter-carrier processes that promote strong competitive outcomes in the telecommunications industry.[112]

72.130 Telstra stated that confining the exception is contrary to the policy behind telecommunications deregulation and could have an adverse impact on the provision of telecommunications services to customers. Telstra noted that a key factor in ensuring seamless interconnection between carriers and carriage service providers has been the disclosure of customer information to enable them to carry and complete calls, form customer relationships and bill customers. Telstra noted some examples of when information needs to be exchanged between carriers or carriage service providers.

> - Where customer A on a carrier's network calls customer B who is on another carrier's network, in order for the call to be put through and completed, and for billing purposes between carriers, the number called plus the calling line identification (CLI) is passed between carriers (together with the customer A's nomination on whether the CLI should be displayed to customer B).

---

108 I Graham, *Submission PR 427*, 9 December 2007.
109 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
110 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.
111 AAPT Ltd, *Submission PR 338*, 7 November 2007.
112 Optus, *Submission PR 532*, 21 December 2007.

- Where a customer of a carrier preselects another carrier as its long distance carrier. The first carrier would need to provide the second with the customer's customer. This would be the case whether or not the customer has a silent line.

- Where a customer of carrier A seeks to move to carrier B for telecommunication services, the customer contacts carrier B to request a transfer of services. Carrier B then contacts carrier A to request the number be ported to carrier A. There are various number portability codes which govern this process. For this process to work seamlessly so that the customer continues to have a working service during this time, certain customer information has to be passed between those carriers.

72.131 Telstra submitted that the inability to continue to work in this manner would have a direct impact on the ability of telecommunications service providers to provide services to customers, and cause delays in the provision of services.[113]

72.132 ACMA and the DBCDE also raised concerns about confining the exception. The DBCDE noted that the exception is critical to maintaining 'any-to-any connectivity' arrangements in telecommunications networks.[114] ACMA submitted that amendment of ss 291 and 302 may result in additional costs, and may narrow the range of services available to all consumers, not only to those who prefer to have their number blocked.[115]

ALRC's view

72.133 The ALRC does not recommend that the exception under ss 291 and 302 of the *Telecommunications Act* should be amended to confine the scope of the exception. The ALRC considered a number of options to confine the exception, but has concluded that these options would be either unworkable in a complex and changing telecommunications environment, or would have unforeseen consequences. The ALRC is concerned that confining the exception may prevent the carriage of communications and the seamless interconnection between carriers and carriage service providers.

72.134 The ALRC acknowledges stakeholder concerns that the exception under ss 291 and 302 may be used to disclose unlisted numbers and other blocked calling numbers. This issue is discussed below.

Specially protected information

72.135 As noted above, some stakeholders raised issues about the use and disclosure of silent numbers, other blocked calling numbers and location information. These issues primarily concerned the exception under ss 291 and 302. This section considers

113 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

114 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

115 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

these issues and whether the *Telecommunications Act* should be amended to protect a category of 'specially protected information'.

Silent numbers and calling number display

72.136 In DP 72, the ALRC noted that Electronic Frontiers Australia had submitted that a number of telecommunications providers have been disclosing calling line identification (CLI) to some of their internet service provider (ISP) customers. CLI reportedly provides these ISPs with caller identification information regardless of whether permanent or per call blocking has been enabled on these lines. That is, the default blocking of calling number display (CND) for unlisted numbers and caller initiated blocking of CND are not operative by virtue of the arrangement of these carriers. [116]

72.137 Electronic Frontiers Australia made a complaint to the Australian Communications Authority (ACA) (now ACMA) and the OPC about telecommunications service providers disclosing CLI to some of their ISP customers. The ACA and the OPC found that some of these disclosures were not permitted under s 291. The OPC decided, however, that in the same circumstances where the ACA found that s 291 was not applicable, carriage service providers could use the s 289(1)(b)(i) exception to disclose information that is not permitted to be disclosed by s 291.[117]

72.138 In DP 72, the ALRC asked whether ss 291 and 302 should be amended to provide that silent and other blocked calling numbers can be used or disclosed only with a person's consent.[118]

72.139 One stakeholder noted that, while it would be ideal to confine the exceptions so that the silent and other blocked calling numbers can be disclosed only with a person's consent, it would not be practical. She noted that there are circumstances in which the disclosure of silent or blocked numbers is necessary for the provision of a requested service to the caller where it is impractical to obtain consent.[119]

72.140 She submitted that the problem arises when silent and other blocked calling number information is disclosed for purposes that are not necessary to connect the call. An example of an inappropriate purpose is when the calling number is disclosed beyond the terminating carrier's call-terminating exchange, and disclosed to the called party. She submitted that such disclosure, without consent, is inappropriate regardless of whether the called party is an individual, business, or a dial-up ISP. She noted that:

> Arguments put forward by those ISPs who contend that receipt of silent and other blocked calling number information is a 'business need' are no different from the

116 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.
117 This issue was also discussed in I Graham, *Submission PR 427*, 9 December 2007.
118 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–4.
119 I Graham, *Submission PR 427*, 9 December 2007.

> arguments that could be put forward by, for example, a non-CSP business such as a dial-up telephone banking service. Dial-up ISP services are not so special that they should have special privileges to receive silent and other blocked calling number information without consent.[120]

72.141 In her view, s 291 should be amended to limit expressly the circumstances when silent and other blocked calling numbers can be used or disclosed. Such circumstances would arise only when it is necessary for the carriage of a telephone communication. She was also concerned that the exceptions under ss 279 and 296 (Performance of person's duties) and s 289(1)(b)(i) (Knowledge of person concerned) may permit the use and disclosure of unlisted or other blocked calling numbers.[121]

72.142 Telecommunications service providers opposed any amendment of the exceptions under Part 13 to limit the use or disclosure of silent or other blocked calling numbers. Optus submitted that limiting s 291 to apply to only listed numbers would have 'disastrous consequences' for the telecommunications industry.[122] Telstra submitted that the disclosure of customer information, including silent numbers, is essential for services to be provided in the telecommunications market. Further, it argued that limiting disclosure of silent and other blocked calling numbers to other carriers or carriage service provides was inappropriate and would be detrimental to the customer. Telstra also noted that calling number display is regulated under an industry code.[123]

Location-based services

72.143 Stakeholders have raised concerns about whether certain exceptions under Part 13 provide adequate protection of location-based information.[124] Location-based services have been used for some time. There are a range of commercially offered location-based services. These are broadly divided into two categories:

- 'active' or 'pull' services that are initiated by an action, such as an SMS, from the consumer requesting that a taxi be sent to the person's present location; and
- 'passive' or 'push' services that are not requested by the consumer.[125]

---

120 Ibid.
121 Ibid.
122 Optus, *Submission PR 532*, 21 December 2007.
123 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2007).
124 I Graham, *Submission PR 427*, 9 December 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.
125 Australian Government Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006).

72.144 Examples of 'active' or 'pull' services would include certain numbers starting with '13' (such as those used by taxi services or food delivery chains) that involve the use of location-based technology, and 'triple 0' emergency calls that capture location information.

72.145 'Passive' or 'push' services may take the form of marketing distributed to consumers according to their whereabouts, or 'tracking' services initiated by third parties interested in the location of other individuals. These services are now offered in Australia, and include:

- Optus 'Friend FindA'. This service enables a person to find out the location of another person's mobile phone if the other person has agreed to share their location with the first person;[126] and

- Telstra's Mobile Location Manager. This service provides location information about Telstra mobile phones and is available to any business or application provider that wishes to 'location enable' their applications.[127]

72.146 The Department of Communications, Information Technology and the Arts (DCITA)[128] considered location-based services in its review of the regulation of content delivered over convergent devices.[129] It noted that the use of active location-based services is likely to be taken as constituting informed consent. The review was concerned, however, that passive location-based services could be misused for illegal or inappropriate purposes if offered without appropriate safeguards.[130]

72.147 DCITA observed that s 291 of the *Telecommunications Act* may operate in certain circumstances to allow for the use and disclosure of location information without a user's consent or knowledge. It suggested that an alternative means of protecting against the privacy and safety issues associated with passive services should be pursued. The review concluded that it would be appropriate to require the consent of an account holder before location information relating to any handsets operated under an account is used or disclosed.[131] It was noted that this approach was consistent with the requirements under the European Union (EU) *Directive Concerning the Processing*

---

126 Optus, 'Friend FindA Help' <www.mobile.optuszoo.com.au> at 23 April 2008.

127 Telstra, 'Mobile Location Manager' <www.telstra.com.au> at 23 April 2008. Telstra also offers a location-based mobile workforce management solution that enables companies to automate employee timesheets, and to monitor job activity and physical location in real time: R Gedda, 'Telstra Launches Mobile Workforce App', CIO (online), 3 November 2006 <www.cio.com.au>, at 23 April 2008.

128 Now the Department of Broadband, Communications and the Digital Economy.

129 Australian Government Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006), 31–32.

130 Ibid, 102.

131 Ibid, 104–105.

of Personal Data and the Protection of Privacy in the Electronic Communications Sector.[132]

72.148 The *Communications Legislation Amendment (Content Services) Act 2007* (Cth) amended s 291 of the *Telecommunications Act* to provide that the use or disclosure by a person of information or a document is permitted if the information or document relates to the location of a mobile telephone handset or any other mobile communications device, and the person has consented to the disclosure or use.[133]

72.149 One stakeholder noted, however, that the amendment did not address the disclosure without consent of mobile phone or device location information to individuals and businesses that are not carriage service providers. She also noted that it is unclear whether the exceptions under ss 279 and 296 (Performance of person's duties) and s 289(1)(b)(i) (Knowledge of person concerned) would allow the disclosure of location information without an individual's consent. She submitted that these exceptions should be amended immediately to provide expressly that the disclosure of location information without consent is prohibited.[134]

A new exception?

72.150 One stakeholder submitted that Part 13 should be amended to establish a category of 'specially protected information' comprising information that is generated, or processed, by a telecommunications network for the purpose of carriage of a communication or billing. This includes information such as calling number information and location information about a mobile phone or other mobile communications device. It was submitted that the protection of this information is particularly important because:

- individuals have no control over the generation of the information, and no way of preventing its use or disclosure unless a means is provided by a telecommunications service provider;

- it is increasingly being used and disclosed for the provision of 'value-added services'; and

---

132 Ibid, 105. See European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002), arts 6–9. While this approach would provide sufficient safeguards to prevent abuse of passive location-based services with respect to adults, DCITA concluded that further measures will be required where services are offered that would identify the location of minors: Australian Government Department of Communications, Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006), 104–105. Communications Alliance also considered privacy issues related to location-based services: Communications Alliance Ltd, *Submission PR 198*, 16 February 2007.

133 *Communications Legislation Amendment (Content Services) Act 2007* (Cth) sch 1, pt 1.

134 I Graham, *Submission PR 427*, 9 December 2007.

- the disclosure of such information without consent is privacy-invasive and potentially puts the safety of an individual at risk.[135]

72.151 It was submitted that the proposed new exception should state that, 'specially protected information' is not permitted to be used or disclosed for any purpose, beyond what is strictly necessary for the transmission of a communication or billing, unless the person has consented to the use or disclosure in the circumstances concerned.[136]

72.152 The stakeholder argued that the exception should state that for the purposes of the exception, consent may be express or implied, and may be taken to be implied only if the service provider has provided the person on a permanent basis with a simple and free of charge means of preventing the use or disclosure of the information. The exception also should state that telecommunications service providers are prohibited from overriding a user's choice to prevent use or disclosure, unless:

- overriding the user's choice to prevent disclosure is necessary to provide the information to a recognised emergency service (for example, an '000' operator);

- the use or disclosure is required or authorised by the *Telecommunications (Interception and Access) Act*; or

- the use or disclosure is necessary for the transmission of a communication or billing.[137]

ALRC's view

72.153 The ALRC is concerned that telecommunications service providers could use the exceptions under ss 291 and 302 of the *Telecommunications Act*, and possibly other exceptions under Part 13, to use or disclose sensitive information such as unlisted numbers, other blocked calling numbers and location information. While the recent amendments to s 291 deal with the use and disclosure of location information between telecommunications service providers, it does not address the use of this information between telecommunications service providers and third parties.

72.154 The ALRC sees merit in an amendment of the *Telecommunications Act* to regulate further the use and disclosure of unlisted numbers, blocked calling number and location information. In particular, the EU and the United Kingdom have recently enacted special laws to deal with the use and disclosure of location information.[138]

---

135 Ibid.
136 Ibid.
137 Ibid.
138 See European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002), arts 6–9; *Privacy and Electronic Communications (EC Directive) Regulations 2003* (UK), r 14.

72.155 The ALRC does not, however, make a recommendation in relation to use or disclosure of unlisted numbers, blocked calling numbers and location information. The ALRC is concerned about any unforeseen consequences of regulating further the use and disclosure of this information. The ALRC has been advised that it may be difficult for telecommunications service providers to comply with laws relating to unlisted or blocked calling numbers. This is because an individual may be a customer of multiple telecommunications service providers, and one provider may not hold the same information about an individual as another. For example, it has been suggested that a telecommunications service provider will not always be aware that a number is unlisted, or that an individual has implemented calling number display blocking.

72.156 These issues should be considered as part of the review of telecommunications legislation recommended in Chapter 71. The ALRC notes that the use and disclosure of information held on the IPND to provide location dependent carriage services is currently being considered by the Australian Government.[139]

Credit reporting information and credit worthiness

72.157 Concerns were raised in a number of submissions about whether Part 13 of the *Telecommunications Act* permitted the use and disclosure of credit information and credit worthiness information that would otherwise not be permitted under the *Privacy Act*.[140]

72.158 Telstra noted that a number of provisions in the *Privacy Act* prohibit disclosure of credit information except where disclosure 'is required or authorised by or under law'.[141] In Telstra's view, a disclosure that falls within one of the exceptions in Part 13 of the *Telecommunications Act* will be 'authorised by law' under Part IIIA and the NPPs in the *Privacy Act*.[142]

72.159 The OPC expressed concern that the exceptions under ss 289, 290 and 291 of the *Telecommunications Act* appear to permit additional use and disclosure in relation to consumer credit.[143] The OPC noted that ACMA has published the following advice on its website:

> Sections 289 and 290 may be relevant to authorise the disclosure of affairs or personal particulars of another person when a carrier or CSP does credit card checks with a credit card company … Section 289 may operate to authorise the disclosure of affairs

---

139 Australian Government Department of Communications, Information Technology and the Arts, *Use of IPND Information to Provide Location Dependent Carriage Services—Discussion Paper* (2007).

140 See, eg, Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

141 *Privacy Act 1988* (Cth) ss 18Q(3), 18Q(5), 18N(1)(g).

142 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

143 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

> or personal particulars of another person in relation to a debt sold to a debt collection agency.[144]

72.160 The OPC submitted that this interpretation of ss 289 and 290 creates two problems.

> First, these exceptions appear to go beyond what a credit provider is permitted to do under the credit reporting provisions in Part IIIA of the *Privacy Act*. However, because of s 303B of the *Telecommunications Act* … such uses and disclosures are taken to be authorised by law for the purposes of the *Privacy Act*, when undertaken by telecommunications businesses covered by Part 13.
>
> Second, sections 289 and 290 appear to create more permissive conditions for use and disclosure of personal information related to consumer credit for those credit providers that operate in the telecommunications sector, compared to those that operate in other industries.[145]

72.161 In DP 72, the ALRC proposed that Part 13 of the *Telecommunications Act* should be amended to provide that use or disclosure by a person of credit reporting information is to be handled in accordance with the *Privacy Act.*[146]

Submissions and consultations

72.162 A number of stakeholders supported the proposal.[147] Telstra stated that it supported the proposal, provided it was limited to 'credit reports' obtained from credit reporting agencies. Telstra argued that it should not apply to billing or payment information of a carrier's customers which should continue to be dealt with under Part 13 of the *Telecommunications Act*.[148] AAPT and Optus submitted that the proposal was unnecessary.[149]

ALRC's view

72.163 Part 13 of the *Telecommunications Act* should be amended to provide that use or disclosure by a person of 'credit reporting information' is to be handled in accordance with the *Privacy Act*. In Chapter 54, the ALRC recommends that 'credit reporting information' should be defined for the purpose of the new *Privacy (Credit Reporting Information) Regulations* as personal information that is:

- maintained by a credit reporting agency in the course of carrying on a credit reporting business; or

---

144 Australian Communications and Media Authority, *Disclosure of Customer Details under Part 13 of the Telecommunications Act 1997 FAQs* <www.acma.gov> at 6 May 2008.

145 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

146 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–6.

147 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

148 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

149 Optus, *Submission PR 532*, 21 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

- held by a credit provider, and has been prepared by a credit reporting agency, and is used, has been used or has the capacity to be used in establishing an individual's eligibility for credit.

72.164 Adverse personal credit listings can have a significant impact on an individual. As outlined in Part G of this Report, the regulation of credit reporting requires a specific level of detail to ensure that credit providers, credit reporting agencies and individuals understand their obligations and rights. The use and disclosure of credit reporting information should not be permitted under ss 289, 290 and 291 of the *Telecommunications Act*. There is no reason why organisations in the telecommunications industry should be subject to more permissive credit reporting rules than organisations in other industries.[150]

Recommendation 72–10 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that use or disclosure by a person of credit reporting information is to be handled in accordance with the *Privacy Act*.

The regulation of public number directories

72.165 This section of the chapter examines the protection of public number directories. It considers the regulation of the IPND and public number directories not sourced from the IPND. The final section discusses whether public number directories are desirable and whether telecommunications service providers should be able to charge for unlisted numbers.

Integrated public number database

72.166 Currently, Telstra's carrier licence requires it to provide and maintain an IPND.[151] The IPND, which was established in 1998, is a database of all listed and unlisted telephone numbers and associated customer data—namely, the name and address of the customer, the customer's service location, the name of the carriage service provider, and whether the telephone is to be used for government, business, charitable or private purposes.[152]

72.167 Telstra reported that the IPND contained 45,999,620 connected records at 30 June 2006, an increase of 2,413,787 records (or 9.5%) over the previous 12 month

150 See Ch 54 for a discussion of 'credit reporting information' and information about the credit worthiness of another person. In that chapter, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'.

151 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

152 Ibid, cl 10(4).

period. At 30 June 2006, 31 carriers and carriage service providers were listed as data providers to the IPND, compared with 24 in the previous 12 month period.[153]

Regulation of the IPND

72.168 Section 472(1) of the *Telecommunications Act* allows the Minister (currently the Minister for Broadband, Communications and the Digital Economy)[154] to determine that a person other than Telstra should provide and maintain an IPND. Any such determination has no effect while Telstra's carrier licence requires it to provide and maintain an IPND.[155] To date, no such determination has been made.

72.169 The *Telecommunications Act* requires carriage service providers to provide Telstra with as much information as is reasonably required to provide and maintain the IPND.[156] Accordingly, disclosure of telecommunications information for inclusion in the IPND is not an offence under Part 13 of the Act because it is 'required or authorised by or under law'.[157]

72.170 The use and disclosure of information in the IPND is subject to Part 13 of the *Telecommunications Act*.[158] Section 285 of the Act allows use or disclosure of IPND information about the affairs or personal particulars of a person for purposes connected with the: provision of directory assistance services by or on behalf of a carriage service provider; publication or maintenance of a directory of public numbers; or the making of a call to an emergency service number.

72.171 Where the *Privacy Act* applies to a person who discloses or uses IPND information, the disclosure or use of such information will not breach the *Privacy Act* so long as the disclosure or use occurs in accordance with Part 13 of the *Telecommunications Act*. That is, the disclosure or use will be authorised by law for the purposes of the *Privacy Act*.[159]

72.172 Telstra's carrier licence also limits the purposes for which information in the IPND can be used and disclosed.[160] It can be disclosed only to a carriage service provider to enable the provider to: provide directory assistance, operator assistance or operator services; produce a public number directory; provide location dependent carriage services; or assist emergency call services and enforcement agencies.[161]

---

153 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 147. At 30 June 2005, 24 carriage service providers provided data to the IPND and the IPND contained approximately 43.6 million records: Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 184.

154 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008, sch, pt 3.

155 *Telecommunications Act 1997* (Cth) s 472(5).

156 Ibid s 101, sch 2, pt 4.

157 Ibid s 280.

158 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, cl 10(9)(b).

159 *Telecommunications Act 1997* (Cth) s 303B.

160 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, cl 10(7).

161 Ibid, cl 10(1).

72.173 In November 2003, the ACA announced its intention to develop an industry standard to articulate clearly the use that may be made of information provided by customers to telecommunications providers. It stated that an industry standard was required because investigations had revealed that information in the IPND was being used for purposes other than those envisaged by Part 13 of the *Telecommunications Act*. These purposes included 'database enhancement', 'data cleansing', 'data verification', and 'list management'.[162]

72.174 In March 2004, the ACA released a discussion paper on regulating the use of IPND data.[163] In May 2005, it released a draft industry standard on the use of IPND data (IPND Draft Standard).[164] Had the IPND Draft Standard been implemented, it would have regulated further the use of IPND data; ensured that customers were aware of the purposes of the collection of IPND data and the purposes for which the information may be disclosed; and enabled customers to choose whether to include their data in a public number directory.

72.175 In December 2006, however, the Australian Parliament passed the *Telecommunications Amendment (Integrated Public Number Database) Act 2006* (Cth) (IPND Act). The IPND Act introduced a definition of 'public number directory' into the *Telecommunications Act* in order to prevent IPND data being used directly for unauthorised purposes, such as the development of reverse search directories, and the production of databases which are used for purposes such as marketing, data cleansing, debt collection, identity verification and credit checking.[165]

72.176 The IPND Act also introduced a new exception to the offence provisions under the *Telecommunications Act* that allows IPND information to be disclosed for specified research purposes that are in the public interest. ACMA has promulgated a *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* that sets out the kinds of research that will be considered to be in the public interest. The public interest research exception is discussed further below.

72.177 Under former arrangements, Telstra, as the IPND Manager, was responsible for deciding applications for access to the IPND for all users. The IPND Act amended the *Telecommunications Act* to provide that IPND data users are required to apply to ACMA for an authorisation to access the IPND. Telstra is permitted to disclose IPND data only to persons holding such an authorisation.

---

162 Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004), 11.

163 Ibid.

164 Australian Communications Authority, *Draft Telecommunications (Use of Integrated Public Number Database) Standard* (2005).

165 *Telecommunications Act 1997* (Cth) s 285(2).

72.178 The IPND Act also requires ACMA to establish a scheme for granting authorisations permitting persons to use and disclose IPND information.[166] The Act requires ACMA to consult with the Privacy Commissioner and Attorney-General's Department on development of the scheme.[167] Criminal sanctions apply for unauthorised secondary disclosure and use of IPND data by public number directory publishers, and for breaches of the conditions of authorisation issued under the IPND scheme.[168] ACMA has established an IPND Scheme under the *Telecommunications Integrated Public Number Database Scheme 2007* and a number of other instruments.[169]

72.179 Information held on the IPND also is regulated under the *Integrated Public Number Database Industry Code of Practice*. Communications Alliance developed this code to reflect better the arrangements outlined in legislation and subordinate instruments, including the IPND Scheme.[170]

Should the IPND be regulated under the *Privacy Act*?

72.180 In DP 72, the ALRC considered whether the IPND should be regulated under the *Privacy Act* rather than the *Telecommunications Act*. The ALRC expressed the preliminary view that the current legislative regime relating to the IPND under the *Telecommunications Act* provides adequate protection of information held under the IPND.[171]

Submissions and consultations

72.181 DCITA submitted that, if only the NPPs were relied upon to govern use and disclosure of IPND information, this would prevent the use and disclosure of IPND information for purposes that are currently permitted under the *Telecommunications Act*. These purposes, it argued, continue to be important for the effective operation of the telecommunications industry, and for public safety.[172]

72.182 DCITA also noted that NPP 2 provides that personal information can be used or disclosed for the secondary purpose of direct marketing if certain criteria are met. It

---

166 Ibid s 295A.
167 Ibid s 295M.
168 Ibid pt 13 div 3A.
169 Including the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* and the *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)*. These instruments are discussed further below.
170 Australian Communications Industry Forum, *Industry Code—Integrated Public Number Database (IPND) Industry Code*, ACIF C555 (2008), [10.7].
171 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [63.112]–[63.116].
172 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007.

submitted that currently IPND information is not permitted to be used for direct marketing purposes and that this prohibition should remain.[173]

72.183 Optus submitted, however, that telecommunications privacy regulation should be moved to the *Privacy Act*, including provisions regulating the IPND. In Optus's view, the additional use and disclosure of IPND information could be accommodated in the *Privacy Act*. It stated that provisions regarding the IPND Manager and requiring carriage service providers to provide data to the IPND should be retained in the *Telecommunications Act*.

72.184 Optus strongly disagreed with DCITA's view that IPND information should not be available for direct marketing purposes. Optus submitted that the current provisions of the *Telecommunications Act* and the *Privacy Act* permit non-IPND directory producers such as Telstra to direct market to the listed customers of all other telecommunications providers. Optus argued that this provides Telstra with a significant competitive advantage. It submitted that restrictions regarding the use or disclosure of telephone directory information should be removed.[174]

ALRC's view

72.185 The privacy aspects of the IPND should continue to be regulated under Part 13 of the *Telecommunications Act*. The IPND is an up-to-date, comprehensive database containing the details of all listed and unlisted telecommunications subscribers. The special nature of the IPND means that a high standard of protection should apply.

72.186 Further, personal information held on the IPND is required to be collected by law, but disclosed and used for purposes not always related to the purpose for which the information was collected. The Australian community is entitled to expect a high level of control over access to that information, and the purposes for which it may be accessed, used and disclosed. The current legislative regime relating to the IPND under the *Telecommunications Act* is appropriate for the protection of information held under the IPND.

Clarifying the provisions that regulate the IPND

72.187 It is unclear to what extent provisions other than s 285 of the *Telecommunications Act* regulate the use or disclosure of information held on the IPND. For example, it is not clear whether all the exceptions under Part 13 apply to IPND information, and how those exceptions interact with Telstra's licence conditions and the *Telecommunications (Interception and Access) Act*.

72.188 Section 285 is the only provision in Part 13 that refers to the IPND. The DBCDE submitted, however, that s 285 is not the only section in Part 13 that permits

173 Ibid.
174 Optus, *Submission PR 532*, 21 December 2007.

access to IPND information.[175] The ALRC has given consideration to the scope of all the exceptions under Part 13 and how they affect the protection of information held in the IPND. None of its recommendations to amend the exemptions under Part 13 would lower the level of protection currently afforded to IPND information.

72.189 It is not clear whether all of the exceptions under Part 13 should apply to the use and disclosure of information contained in the IPND. In particular, the ALRC is concerned that s 289(1)(b)(i) would allow the use and disclosure of IPND information for a broad range of purposes. This should be the subject of further consideration by the Australian Government.

72.190 How the exceptions under Part 13 interact with Telstra's carrier licence also is unclear. Telstra's carrier licence provides that it must establish and maintain the IPND to provide information for a range of purposes, including purposes connected with 'providing location dependent carriage services'.[176] It is unclear whether this condition is consistent with Part 13. The exception under s 291 permits the disclosure of information or a document that relates to the location of a mobile telephone handset or other mobile communications device if a person consents to that disclosure. None of the exceptions under Part 13, however, state that information held on the IPND can be disclosed for this purpose.

72.191 Two stakeholders submitted that s 285 should be amended to clarify that IPND information may be used for the provision of location-dependent carriage services.[177] Another stakeholder was strongly opposed to any proposal to permit additional uses or disclosures of information for such purposes.[178] The Australian Government is currently considering this issue.[179]

72.192 As noted above, the *Telecommunications (Interception and Access) Amendment Act* deleted the law enforcement and protection of public revenue provisions from Part 13 of the *Telecommunications Act* and introduced a new Chapter 4 into the *Telecommunications (Interception and Access) Act*. Chapter 4 regulates the use and disclosure of 'telecommunications data' for the purpose of assisting the Australian Security Intelligence Organisation (ASIO) and other law enforcement and intelligence agencies. The Act does not set out a definition of 'telecommunications data'. It is unclear therefore whether these provisions regulate the use and disclosure of information held on the IPND.

---

175 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

176 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* cl 10(1)(d).

177 Optus, *Submission PR 532*, 21 December 2007; Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

178 I Graham, *Submission PR 427*, 9 December 2007.

179 Australian Government Department of Communications, Information Technology and the Arts, *Use of IPND Information to Provide Location Dependent Carriage Services—Discussion Paper* (2007).

72.193 Part 13 should be amended to clarify when a use or disclosure of information or a document held on the IPND is permitted. This amendment should set out which provisions under Part 13 regulate the use and disclosure of IPND information, and how they interact with Telstra's licence conditions and the *Telecommunications (Interception and Access) Act*.

Recommendation 72–11 The *Telecommunications Act 1997* (Cth) should be amended to clarify when a use or disclosure of information or a document held on the integrated public number database is permitted.

Enforcement agency

72.194 The *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (Cth) provides that Telstra must establish and maintain an IPND[180] to provide information for purposes connected with a number of activities, including 'assisting enforcement agencies'.[181] The Declaration provides that the definition of 'enforcement agency' has the same meaning given by s 282 of the *Telecommunications Act*.[182]

72.195 Section 282 was recently repealed by the *Telecommunications (Interception and Access) Amendment Act 2007*.[183] The section defined 'enforcement agency' as a:

- criminal law enforcement agency (including the Australian Federal Police; a police force or service of a state or a territory; the Australian Commission for Law Enforcement Integrity; the Australian Crime Commission; the NSW Crime Commission; the Independent Commission Against Corruption of NSW; the Crime and Misconduct Commission of Queensland; and a prescribed authority established by or under a law of the Commonwealth, a state or territory);

- civil penalty enforcement agency (an agency responsible for administering a law imposing a pecuniary penalty); or

- public revenue agency (an agency responsible for the administration of a law relating to the protection of the public revenue, including the Australian Taxation Office).

---

180 The integrated public number database is discussed in Ch 72.

181 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (Cth) cl 10.

182 Ibid cl 3.

183 The section provided that the use or disclosure by a person of information is not prohibited if the use or disclosure is reasonably necessary for certain law enforcement purposes, including the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty or the protection of public revenue: *Telecommunications Act 1997* (Cth) s 282(1), (2).

72.196 Section 282 was replaced by Chapter 4 of the *Telecommunications (Interception and Access) Act*. The *Telecommunications (Interception and Access) Act* regulates interception and access by ASIO and enforcement agencies. 'Enforcement agency' is defined in the *Telecommunications (Interception and Access) Act* in almost identical terms to s 282 of the *Telecommunications Act*. The only difference is that the definition in the *Telecommunications (Interception and Access) Act* includes a number of agencies in state anti-corruption agencies that were not established at the time that s 282 was first enacted.

72.197 All the agencies included in the definition of 'enforcement agency' under the *Telecommunications (Interception and Access) Act* should be permitted to access information held on the IPND. Each of these agencies is subject to oversight by the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or state and territory equivalents. Such an amendment would ensure consistency between the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration* and the *Telecommunications (Interception and Access) Act*. The ALRC therefore recommends that the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration* should be amended to provide that 'enforcement agency' has the same meaning as that provided for in the *Telecommunications (Interception and Access) Act*.

Recommendation 72–12 Clause 3 of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (Cth) should be amended to provide that 'enforcement agency' has the same meaning as that provided for in the *Telecommunications (Interception and Access) Act 1979* (Cth).

Emergency service numbers

72.198 Section 285 currently restricts the permitted use and disclosure of IPND information for the purpose of emergency call services to listed numbers. Optus submitted that s 285 should be revised to clarify that both unlisted and listed numbers can be used and disclosed for matters raised by a call to an emergency service number.[184]

72.199 Most individuals would reasonably expect the disclosure of an unlisted number in an emergency call situation. The ALRC recommends therefore that, in the interest of the health and safety of individuals, the *Telecommunications Act* should permit the disclosure of an unlisted number contained in the IPND if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.

184 Optus, *Submission PR 532*, 21 December 2007.

Recommendation 72–13 Section 285 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a disclosure of an unlisted number is permitted if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.

Research exception

72.200 Sections 285(1A)(c)(iv) and 285(1A)(d) of the *Telecommunications Act* provide an exception to the prohibition on use and disclosure of information contained in the IPND. If the disclosure is made to another person for purposes connected with the conduct of research of a kind specified in an instrument under s 285(3), and the other person has been authorised by ACMA to use and disclose the information, such access is permitted. Section 285(3) provides that the Minister may, by legislative instrument, specify the types of research that are in the public interest.

72.201 On 4 May 2007, the Minister for Communications, Information Technology, and the Arts issued the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* (Cth). The Instrument provides that permitted research for the purposes of s 285(1A)(c)(iv) includes:

- research, or the compilation or analysis of statistics, relevant to public health, including epidemiological research, where the research is not conducted primarily for a commercial purpose;

- research regarding an electoral matter conducted by a registered political party, a political representative, a candidate in an election for a parliament or a local government authority or a person on behalf of such a party, representative or candidate, where the research is not conducted primarily for a commercial purpose; and

- research conducted by or on behalf of the Commonwealth, a Commonwealth authority or a prescribed agency which will contribute to the development of public policy, where the research is not conducted for a primarily commercial purpose.[185]

72.202 The OPC submitted that the research exception may be interpreted too broadly. The OPC suggested that particular terms should be defined in the Act itself.

185 *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* (Cth). A 'prescribed FMA agency' is a body, organisation or group mentioned in the *Financial Management and Accountability Regulations 1997* (Cth) sch 1.

Such terms include: what constitutes research in the public interest; and, in terms of medical research, what would be considered 'non-commercial use'.[186]

72.203 A key concept in each of these categories is that the research 'is not conducted for a primarily commercial purpose'. This is in contrast to the National Health and Medical Research Council guidelines made under ss 95 and 95A of the *Privacy Act*.[187] These guidelines provide that where research may breach the IPPs or NPPs, the research must be approved by a Human Research Ethics Committee (HREC). Before approving a particular research proposal under the guidelines, an HREC is required to consider whether the public interest in the research *substantially outweighs* the public interest in the protection of privacy.[188]

72.204 In DP 72, the ALRC proposed that the test under the ss 95 and 95A guidelines be amended to provide that, before approving an activity, an HREC must be satisfied that the public interest in the activity *outweighs* the public interest in maintaining the level of privacy protection provided by the proposed UPPs. The ALRC also expressed the preliminary view that this was the appropriate test in relation to the use and disclosure of information contained in the IPND for the purpose of research in the public interest.

72.205 The ALRC therefore proposed that the Australian Government should amend the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument* to provide that the test of research in the public interest is met when the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the IPND.[189]

Submissions and consultations

72.206 The DBCDE submitted that it would not be appropriate to amend the *Telecommunications (Integrated Public Number Database-Permitted Research Purposes) Instrument*, as the Minister is required to decide whether the research is in the public interest.[190]

72.207 Other stakeholders provided qualified support for the proposal. The OPC supported the ALRC's proposal but submitted that, given that individuals have no

---

186 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

187 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000); National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

188 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), guideline 3.2; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), guideline D.4.

189 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–7.

190 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

choice as to whether their personal information is included in the IPND, any research proposal that lessens privacy should demonstrate that the public interest in the research proposal 'substantially' outweighs the public interest in maintaining the level of protection afforded in the IPND.[191]

72.208 The Australian Privacy Foundation supported the proposal, provided an appropriate ethics committee is either identified or established to make independent assessments of the balance of interests. The Foundation also noted that the ALRC does not address the weakness of the definition of research in the IPND scheme, which includes such activities as political canvassing which, it argued, should not be able to take advantage of the exception.[192]

ALRC's view

72.209 The Australian Government should amend s 285(3) of the *Telecommunications Act* to provide that before the Minister specifies types of research for the purpose of the use or disclosure of information or a document contained in the IPND, the Minister must be satisfied that the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the IPND.[193]

72.210 The appropriate test is whether the public interest in the relevant research outweighs the public interest in maintaining the protection of the personal information held on the IPND. Consideration of whether a research project is for a commercial purpose is not the appropriate test. It will not always be clear when research primarily is conducted for a commercial purpose. Further, research that is clearly in the public interest may also have a commercial purpose.

72.211 The ALRC notes that all research conducted pursuant to the recommended research exception under the *Privacy Act* must be reviewed by an HREC which must apply the public interest test. The ALRC does not recommend the establishment of an ethics committee to make independent assessments of the balance of interests, however, the DBCDE may want to consider this mechanism when next reviewing the *Telecommunications (Integrated Public Number Database-Permitted Research Purposes) Instrument.*

72.212 The ALRC is concerned about the use of IPND information for research regarding an electoral matter conducted by a registered political party, a political representative, a candidate in an election for a parliament or a local government

191 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

192 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also I Graham, *Submission PR 427*, 9 December 2007.

193 The public interest test is discussed in detail in Ch 65.

authority. Those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community.[194]

72.213 The ALRC is particularly concerned that this provision would allow the use of IPND information for a range of activities, including political canvassing. The DBCDE should monitor the use of IPND information for research regarding electoral matters, and should consider whether IPND information should continue to be used for this purpose when next reviewing the *Telecommunications (Integrated Public Number Database-Permitted Research Purposes) Instrument*.

Recommendation 72–14 The Australian Government should amend s 285(3) of the *Telecommunications Act 1997* (Cth) to provide that before the Minister specifies a kind of research for the purpose of the use or disclosure of information or a document contained in the Integrated Public Number Database, the Minister must be satisfied that the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the Integrated Public Number Database.

Notifying the Privacy Commissioner of a breach

72.214 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* sets out the conditions upon which ACMA may grant authorisations for access to information contained in the IPND under the IPND scheme.

72.215 Clause 6 of the Determination provides that an authorisation under the IPND scheme is subject to a condition requiring the holder of the authorisation, as soon as practicable after the holder becomes aware of a substantive or systemic breach of security that could reasonably be regarded as having an adverse impact on the integrity and confidentiality of the protected information, to notify ACMA and the IPND Manager, and to take reasonable steps to minimise the effects of the breach. This obligation is reflected in the *Integrated Public Number Database Industry Code of Practice*—a code developed by Communications Alliance and registered with ACMA.[195]

72.216 In DP 72, the ALRC proposed that the *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination* should be amended to provide that an authorisation under the IPND scheme is subject to a

194 See Ch 41.

195 Australian Communications Industry Forum, *Industry Code—Integrated Public Number Database (IPND) Industry Code*, ACIF C555 (2008), [10.7].

condition requiring the holder of the authorisation to notify the OPC, as soon as practicable after becoming aware:

- of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of the protected information; and

- that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.[196]

Submissions and consultations

72.217 A number of stakeholders supported the proposal.[197] For example, the DBCDE expressed support for the proposal on the basis that a substantive or systemic breach of security that impacts on the integrity and confidentiality of personal information could potentially be a breach of the *Privacy Act* as well as the *Telecommunications Act*.[198] Optus did not support the proposal because the *Integrated Public Number Database Industry Code of Practice* already contains procedures to be followed by an IPND data user.[199]

ALRC's view

72.218 The holder of an authorisation should be required to notify the OPC as soon as practicable after the holder becomes aware of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of the protected information. It is important that the OPC be given an opportunity to investigate whether a breach of security has also resulted in an interference with an individual's privacy. This requirement is consistent with the ALRC's recommendation relating to data breach notification.[200]

72.219 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination* and the *Integrated Public Number Database Industry Code of Practice* require the user of IPND information to inform the

---

196 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–8.

197 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

198 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

199 Optus, *Submission PR 532*, 21 December 2007.

200 In Ch 51, the ALRC recommends that the *Privacy Act* should be amended to include a new Part on data breach notification, which will provide that an agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

IPND Manager of a breach. In the ALRC's view, because the holder of an authorisation may use personal information held on the IPND for purposes that are not related to the purpose of collection, it is appropriate that they are under an additional obligation to notify the OPC of a suspected breach of security or contravention of a legal restriction.

Recommendation 72–15 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Privacy Commissioner, as soon as practicable after becoming aware:

(a) of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of protected information; and

(b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.

Public number directories not sourced from the IPND

72.220 The ACA has noted that Telstra's directory arm, Sensis, has a database of information provided to it by other telecommunications providers under bilateral agreements. This enables Sensis to publish the White Pages based on this information, rather than from information sourced from the IPND.[201] Consequently, Sensis is not subject to the IPND provisions under the *Telecommunications Act*.

72.221 It is unclear what rules apply to information collected by Sensis for inclusion in the White Pages. This information may be regulated under Part 13 of the *Telecommunications Act* and the *Privacy Act*. It could be argued, however, that it is not regulated under Part 13. Information collected from other carriage service providers subject to bilateral agreements is not information that comes to Sensis's knowledge, or into its possession, in connection with its business as a carrier or carriage service provider.[202] Further, it could be argued that neither Telstra nor Sensis is an 'eligible number-database person'. Personal information collected for inclusion in the White Pages, therefore, may be regulated by the *Privacy Act* alone, which would allow Telstra to use that information for purposes such as direct marketing.

---

201 Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004), 8.

202 See *Telecommunications Act 1997* (Cth) s 276.

72.222 In DP 72, the ALRC noted that stakeholders were concerned that publishers of public number directories that do not use the IPND are not regulated adequately. ACMA stated that this was a key concern highlighted in submissions to the IPND Draft Standard.[203] It was noted that the IPND Act amendments to the *Telecommunications Act* will not affect publishers of public number directories that do not use the IPND.[204] A number of stakeholders suggested that directory publishers should be subject to the same regulatory standards, regardless of the source of the data.[205]

72.223 It also was submitted that the current regulatory scheme results in an 'uneven playing field' and huge gaps in the protection of personal information.[206] In particular, it was noted that there is no prohibition on directory publishers producing directories which are not sourced from the IPND and that are reverse-searchable.[207] ACMA noted that it routinely receives complaints from the community about the existence of reverse search directories. ACMA is unable to take action to shut down a reverse search directory where the data comes from another source, or if it cannot establish that IPND customer data is the source used.[208]

72.224 In DP 72, the ALRC asked whether directory products that are produced from data sources other than the IPND should be subject to the same rules under Part 13 of the *Telecommunications Act* as directory products which are produced from data sourced from the IPND.[209]

Submissions and consultations

72.225 A number of stakeholders answered the question in the affirmative.[210] For example, ACMA submitted that it is the community's expectation that all telephone directories should be subject to the same rules, independent of the source of the data used for the directory.[211] The DBCDE submitted that there are strong arguments on competition and privacy grounds that all directory publishers be regulated in the same manner, regardless of where or how they source their information.[212] The Australian

---

203 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

204 Ibid; Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

205 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007; Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007.

206 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

207 Australian Government Department of Communications, Information Technology and the Arts, *Submission PR 264*, 22 March 2007. A reverse-search telephone directory allows users to search by a telephone number to retrieve the customer details for that service.

208 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

209 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–5.

210 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

211 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

212 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

Finance Conference submitted that there appears to be no reason to distinguish the compliance requirements for producers of directories from either the IPND or another source, and that the compliance requirements should be uniform.[213]

72.226 Optus submitted that the current arrangement gives Telstra an unfair competitive advantage in that it can direct market to everybody on its directory while others who only have access to the IPND are not able to. Optus also submitted that listed numbers are publicly available information and should be available to all who want to use it. Optus argued that directory producers should be allowed to use this information freely and apply current technology to it, including reverse search directories and predictive diallers. Optus also submitted, however, that if it is deemed necessary to retain the new IPND regulations, then they must apply equally to all directory producers including directory products.[214]

72.227 Telstra, however, maintained that products that are produced from data sources other than the IPND should not be subject to the same rules as directory products produced from data sourced from the IPND.

> The IPND should be the subject of special regulation because it is mandatory to contribute customer information to the IPND. That is, inclusion of customer information in the IPND is not optional. This should be distinguished from customer information, such as that used by Sensis, which is obtained by agreement directly from telecommunications companies and customers.[215]

72.228 Telstra submitted that the fact that data is obtained by Sensis directly from telecommunications companies and customers does not mean that such data is not afforded protection or that there is any 'gap' in the protection of that data. It also noted that Telstra and Sensis are subject to regulatory requirements under Part 13 of the *Telecommunications Act* and the *Privacy Act*. Telstra submitted that the *Telecommunications Act* prohibits the production of a reverse search directory from data sourced under the *Telecommunications Act* without the consent or knowledge of the people concerned.

> In Telstra's view section 289 only permits disclosure of information if the person to whom that information relates consented to the disclosure or was reasonably likely to have been aware or made aware that information was usually disclosed or used in the circumstances concerned. Telstra believes that this exception would allow the production of a public number directory, but not extend to the production of a reverse search directory unless those concerned provided their consent or were reasonably likely to be aware that their information would be used in that way. [216]

72.229 Telstra also submitted that further regulation on directory producers such as Sensis will not prevent the illegal copying of directory information and the production

---

213 Australian Finance Conference, *Submission PR 398*, 7 December 2007.
214 Optus, *Submission PR 532*, 21 December 2007.
215 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
216 Ibid.

of reverse search directories based on that data. Telstra also noted that neither Telstra nor Sensis 'on sell' White Pages directory data to any third parties.[217]

ALRC's view

72.230 The ALRC is concerned that two sets of rules apply to essentially the same information. The ALRC can see no reason why public directory producers should be subject to different compliance requirements based on the source of the information. While the ALRC agrees that one of the reasons why the IPND should be subject to special regulation is because it is mandatory to contribute customer information to the IPND, this does not justify information held on the White Pages being subject to less stringent protection. Further, while the ALRC has not heard that information held on the White Pages is being used inappropriately, the ALRC is concerned that information held on the database could be used for purposes unrelated to the provision of public directory services such as direct marketing, data cleansing and reverse search directories.

72.231 It is a principle of privacy laws that the use and disclosure of personal information for a purpose other than the primary purpose of collection (the secondary purpose) generally should be related to the primary purpose of collection. The use and disclosure of personal information held on the White Pages for a secondary purpose should be subject to the same restrictions imposed on information held on the IPND. Both the IPND and White Pages information are up-to-date, comprehensive databases containing the details of all listed (and in the case of the IPND, unlisted) telecommunications subscribers. Both databases justify special rules to ensure that information held on them is handled according to accepted privacy principles.

72.232 There also is a lack of certainty as to what rules currently regulate the use and disclosure of information contained in the White Pages. This uncertainty should be clarified. The *Telecommunications Act* should be amended to provide that directory products that are produced from data sources other than the IPND should be subject to the same rules under Part 13 of the *Telecommunications Act* as directory products which are produced from data sourced from the IPND.

Recommendation 72–16 The *Telecommunications Act 1997* (Cth) should be amended to provide that directory products that are produced from data sources other than the Integrated Public Number Database should be subject to the same rules under Part 13 of the *Telecommunications Act* as directory products which are produced from data sourced from the Integrated Public Number Database.

217 Ibid.

Are public number directories desirable?

72.233 A significant issue for consideration is whether public number directories that contain contact details of residential consumers are still desirable. In DP 72, the ALRC noted that ACMA had submitted that, given the proliferation of mobile phones and the corresponding lack of mobile phone directories, it may be that the community sees decreasing benefit in public number directories. This would especially be the case for non-business users. Many individuals now prefer to limit the provision of their information, rather than have it publicly available.[218]

72.234 The Australian Institute of Mercantile Agents submitted, however, that public number directories should be more readily available.

> The IPND directories must be regarded as allowable public information. This is the only source of locator information our members have access to and yet availability of this data continually is challenged … Our industry is under the constant threat of banning access to information for debt collection purposes. The only persons assisted by such heavy handed misguided intervention are those who do not meet their contractual obligations.[219]

72.235 The ALRC does not have a view on whether public number directories are still desirable. It is clearly important, however, that subscribers to telecommunications services are informed that their personal information will be included in a public directory. It is unnecessary to provide for this duty in the *Telecommunications Act*, as the issue is dealt with adequately under the *Privacy Act*.[220] Further, in Chapter 73, the ALRC recommends that ACMA, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry. This guidance should address a telecommunications supplier's obligation to inform an individual that their personal information may be included in a public number directory.

Charging a fee for an unlisted number

72.236 The *Telecommunications Act* provides that an unlisted number cannot be disclosed except in specified contexts.[221] The Act is silent on whether a fee can be charged for an unlisted number. The *Carrier Licence Conditions (Telstra Corporation Limited) Declaration* defines an unlisted number as a public number that is one of the following kinds:

---

218 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

219 Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007. See also Australian Finance Conference, *Submission PR 294*, 18 May 2007.

220 The telecommunications industry is currently subject to NPP 1.3, which requires an organisation at or before the time it collects personal information from the individual to take reasonable steps to ensure that the individual is aware of the purposes for which the information is collected. NPP 5 requires an organisation to set out in a document clearly expressed policies on its management of personal information. This obligation would require a telecommunications supplier to indicate to individuals that their personal information may be included in a public directory.

221 *Telecommunications Act 1997* (Cth) ss 276(1)(a)(iv), 277(1)(a)(ii), 285(1)(a), 285(2).

- a mobile number, unless the customer and the carriage service provider that provides the mobile service to the customer agree that the number will be listed;
- a geographic number that the customer and the carriage service provider that provides services for originating or terminating carriage services to the customer agree will not be included in the directory;
- the number of a public payphone; or
- a number that, when dialled, gives access to a private telephone exchange extension that the customer has requested not be included in the directory.[222]

72.237 Article 12.2 of the EU *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* provides that a fee should not be charged for an unlisted number:

> Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.[223]

72.238 ACMA has noted that some stakeholders making submissions to it in relation to its Draft IPND Standard suggested that the imposition of a fee may impact on a consumer's decision to choose to have an unlisted number. Consumers have queried whether such a fee contravenes the *Privacy Act*, and asked why a fee is imposed for an unlisted fixed line number, but not for mobile services.[224]

72.239 In its submission to ACMA on the Draft IPND Standard, the OPC noted that:

> One of the stated objects of the draft standard (clause 5(d)) is that an individual 'may choose whether his or her customer data is to be included in a public number directory'. A relevant question then is whether it is appropriate for individuals to be expected to pay for the right to make privacy choices. Charging a fee for a silent number or to make other choices may limit some individuals' ability to make such choices freely, and thereby hamper their ability to control their own personal information. The effect that free silent listings may have on the number of individuals that appear in directories of public numbers may also need to be considered.[225]

72.240 In DP 72, the ALRC expressed the view that, while charging for an unlisted number may not be a breach of NPP 8, it reduces an individual's ability to control the

---

222 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, cl 3.

223 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002).

224 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

225 Office of the Privacy Commissioner, *Submission to Telecommunications (Use of Integrated Public Number Database) Draft Industry Standard 2005*, August 2005.

use or disclosure of their personal information. Many people request an unlisted number because of safety concerns or because they do not wish to be contacted by telemarketers.[226] The ALRC therefore proposed that the *Telecommunications Act* be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.[227]

Submissions and consultations

72.241 A number of stakeholders supported this proposal.[228] For example, the OPC submitted that:

> The Office receives a number of enquiries and some complaints from members of the public who object to the payment of a fee to exercise their choice of being unlisted in the public telephone directory. The Office takes the view that charging a fee for a silent number may affect individuals' ability to make such choices freely, and thereby hamper their ability to control their own personal information. This may be particularly the case in regard to individuals on low or fixed incomes.[229]

72.242 The Federation of Community Legal Centres (Vic) supported the proposal, and submitted that such an amendment would be consistent with the recognition in the *Privacy Act* that privacy is a human right and that persons asserting such a right should be able to do so with as little effort or inconvenience as possible.

> In particular, the proposed amendment recognises the needs of our clients who are experiencing or have experienced family violence, and who need to ensure, in as simple and effective a manner as possible, that the perpetrator is unable to contact them by telephone.[230]

72.243 ACMA submitted that it understands that consumer expectations of the benefits of having an unlisted number go beyond the mere omission of the number from public number directories. For example, having an unlisted number has meant that a consumer's CND is blocked and that their details cannot be disclosed from the IPND for publication in a public number directory or for use by a researcher in a research project. ACMA also suggested that individuals may not be aware of what exactly they are paying for by having an unlisted number. Further, it submitted that it is unclear what administrative costs the fee is intended to cover—particularly given there is no such fee for mobile phone services.[231]

---

226 A number of respondents to the ALRC's National Privacy Phone-In on 1–2 June 2006 noted that they had unlisted numbers to avoid telemarketers. See Ch 1 for discussion of the National Privacy Phone-In.

227 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 63–9.

228 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Confidential, *Submission PR 535*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

229 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

230 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007.

231 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

72.244 The DBCDE submitted that the proposal will have commercial implications for the White Pages and other telephone directories.

> Not charging for an unlisted number might result in a considerable increase in the proportion of residential telephone service users having unlisted numbers. If this were to occur, the number of entries in the printed and electronic White Pages and other telephone directories, and therefore their usefulness, would be reduced. It is possible that telephone directories could eventually become redundant, although this does not appear to have been the case in the European experience.[232]

72.245 Telstra strongly objected to the proposal for a number of reasons. First, it noted that the ALRC had referred to the EU *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, but noted that the ALRC had not considered other comparable jurisdictions, such as the United States, Canada and Singapore, where customers are charged for unlisted numbers.

72.246 Telstra noted that while some individuals may want a silent line to reduce their telemarketing calls, the ALRC should acknowledge the impact of the introduction of the Do Not Call Register, existing protections against telemarketing under the *Telecommunications Act* and the *Privacy Act*, and that the White Pages Online site is protected from unauthorised downloads of data.

72.247 It was submitted that the Australian telecommunications market is fiercely competitive, and that consumers can choose a telecommunications service provider that does not charge for the service. Telstra submitted that there is no market failure which leads to a need for the price to be regulated or the fee removed.

72.248 Telstra submitted that the ALRC did not present any evidence to suggest that individuals' safety is compromised by the charge for an unlisted number. It noted that a silent line is one aspect of an individual's approach to the management of their security. In the period since July 2005, Telstra reported that it has received only three complaints with respect to the existence of a charge for silent lines. It submitted that this supports the view that customers see the value in the service and do not believe that the charge is too high or compromises safety.

72.249 Telstra noted that its unlisted number service is a commercial service offered by a privately-owned company, and that its investors expect a competitive return on their investment. It observed that it carries a consequent commercial, reputational and financial risk and incurs costs to provide and maintain the service. These costs include those of: employing personnel to enter and process data, maintaining information technology systems, and responding to customer requests; updating the database to avoid unauthorised disclosure; information technology and systems; and undertaking

---

232 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

sophisticated verification procedures to reduce the mistaken release of silent line information.

72.250 It was submitted that the current fee is nominal. The fee has been maintained at a nominal GST-exclusive price of $2.66 per month for more than 12 years. Telstra has not increased this fee.[233]

72.251 Telstra argued that the fee is targeted correctly to the users of the service, and that it is unreasonable that its customers or shareholders should be asked to subsidise the services for consumers who wish to take additional steps to protect their personal security. It argued that, if one of the arguments in favour of this proposal is to meet the needs of the financially disadvantaged, this is a matter for a government subsidy and not an appropriate basis on which to recommend that charging of a fee for an unlisted number on a public number directory should be prohibited.

72.252 Telstra's carrier licence requires it to publish a public number print directory. It argued that the comprehensiveness of the White Pages directory is important to enable Telstra to comply with other statutory and regulatory obligations, such as the obligation to provide directory assistance services. As a result, its systems and processes are geared toward including a customer's details in the White Pages directory and related products and services, to maximise the comprehensiveness of the White Pages directory.

72.253 Telstra also argued that the issue of charging for an unlisted number has been considered and rejected by appropriate regulatory bodies, including ACMA. It also submitted that the proposal ignores specific elements of the Terms of Reference for the current Inquiry, particularly the requirement that the ALRC consider 'the desirability of minimising the regulatory burden on business in this area'.[234]

ALRC's view

72.254 As has been noted throughout this Report, privacy is recognised internationally as a human right. This also is reflected in the Preamble to the *Privacy Act*, which makes reference to human rights, and specifically to those guaranteed in the *International Covenant on Civil and Political Rights*.[235]

72.255 The Preamble to the *Privacy Act* also refers to Australia's obligations at international law 'to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence' and to protect 'privacy and individual liberties'. While charging for an unlisted number is not a breach of NPP 8, it is a financial impediment to accessing a service that will help to

---

233 CPI indexation for this period would have taken the GST exclusive price to $3.80 per month: Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

234 Ibid.

235 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

protect privacy. A charge reduces an individual's ability to control the use or disclosure of their personal information. This is particularly an issue for individuals on fixed or low incomes.

72.256 While the the EU *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* provides that a fee should not be charged for an unlisted number, other jurisdictions do not prohibit the charging of fee. This is not, however, an argument against prohibiting the charging of a fee for an unlisted number. In DP 72, the ALRC cited the EU as an example of a jurisdiction that has chosen to prohibit the charging of a fee for an unlisted number, not in support of such a prohibition. The ALRC has not been able to find any information to suggest that the EU Directive has unreasonably disadvantaged European telecommunications service providers or has resulted in telephone directories becoming redundant.

72.257 The ALRC also acknowledges Telstra's argument that the prohibition on charging a fee would prevent it from satisfying its licence conditions. A ban on a fee for unlisted numbers may result in less people choosing to be included in a public telephone directory. While the result of this recommendation may be that public number directories are less comprehensive, it would not prevent Telstra providing directory assistance services or producing a White Pages directory.

72.258 The ALRC notes Telstra's arguments that it has received only three complaints with respect to the existence of a charge for silent lines, and that Telstra cites this as supporting the view that customers don't believe that the charge is unreasonable or compromises safety. The OPC submitted, however, that it receives a number of enquiries and some complaints from members of the public who object to the payment of a fee to exercise their choice of being unlisted in the public telephone directory. The ALRC also is concerned about the needs of those who have experienced family violence, and who need to ensure that the perpetrator is unable to contact them. This is not a privacy protection for which an individual in such a situation should be charged.

Recommendation 72–17 The *Telecommunications Act 1997* (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

73. Other Telecommunications Privacy Issues

Contents

Introduction

73.1 Chapters 71 and 72 considered the *Telecommunications Act 1997* (Cth) and how it interacts with the *Privacy Act 1988* (Cth). This chapter examines a number of other privacy-related telecommunications issues. The first section of the chapter examines access to, and interception of, information under the *Telecommunications (Interception and Access) Act 1979* (Cth). The next section looks at the regulation of spam and telemarketing under the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).[1] The final section considers cooperation between the various bodies with responsibility for privacy in the telecommunications industry.

Interception and access

73.2 Laws relating to the interception of telecommunications were initially concerned with preserving the integrity of telecommunication systems.[2] In 1960, however, the *Telephonic Communications (Interception) Act 1960* (Cth) was introduced to protect the privacy of individuals by making it an offence to intercept communications passing over telecommunication systems (with certain exceptions).[3] In 1979, this Act, and other legislation governing the interception of telecommunications, was repealed and replaced with the *Telecommunications (Interception) Act 1979* (Cth).[4] Since then, there have been a number of inquiries into telecommunications interception and numerous changes to interception legislation.[5]

73.3 The *Telecommunications (Interception) Amendment Act 2006* (Cth) amended the *Telecommunications (Interception) Act* to change the name of the Act to the *Telecommunications (Interception and Access) Act 1979* (Cth). The 2006 amendments also implemented a number of the recommendations of the *Report of the Review of the Regulation of Access to Communications*, conducted by Mr Anthony Blunn (the Blunn Report).[6]

---

1 Direct marketing is discussed more generally in Ch 26.
2 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [753].
3 *Telephonic Communications (Interception) Act 1960* (Cth).
4 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [754]–[755].
5 See, eg, A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department; D Stewart, *Report of the Royal Commission of Inquiry into Alleged Telephone Interceptions* (1986) Australian Government; Parliament of Australia—Joint Select Committee on Telecommunications Interception, *Report* (1986).
6 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department. Mr Blunn is a former Secretary of the Attorney-General's Department.

73.4 The Blunn Report concluded that there was inadequate regulation of access to stored communications, as well as insufficient protection of privacy during the access, storage and disposal processes of stored communications.[7] The *Telecommunications (Interception) Amendment Act* expanded the regulatory telecommunications interceptions scheme by prohibiting access to stored communications, subject to a number of exceptions. It also introduced a regime for the use, disclosure, retention and destruction of accessed stored communications.[8]

73.5 The 2006 amendments broadened the exceptions to prohibited interceptions by introducing 'B-Party' warrants. B-Party warrants are directed to innocent third parties (a 'B-Party') who are likely to communicate with individuals under investigation for serious offences.[9] These controversial amendments are discussed below.

73.6 The Blunn Report also concluded that the distribution of provisions between the *Telecommunications Act* and the *Telecommunications (Interception) Act* (as it was then known) dealing with access to telecommunications data for security and law enforcement purposes was 'complicated, confusing and dysfunctional'.[10] The report recommended the introduction of comprehensive legislation dealing with access to all telecommunications and telecommunications data for law enforcement and security purposes.[11]

73.7 The *Telecommunications (Interception and Access) Amendment Act 2007* (Cth) implemented this recommendation. The 2007 amendments removed provisions relating to the use and disclosure of information and documents for law enforcement and security purposes from Part 13 of the *Telecommunications Act*, and introduced a new Chapter 4 into the *Telecommunications (Interception and Access) Act*. Chapter 4 sets out a regime for particular officers of ASIO or an enforcement agency to authorise telecommunications service providers to disclose 'telecommunications data' without breaching the offence provisions under the *Telecommunications Act*.[12] These amendments are discussed below.

73.8 The ALRC's current Inquiry is focused on the extent to which the *Privacy Act* and related laws provide an effective framework for the protection of privacy in Australia. As discussed in Chapter 1, communications interception generally is an issue that is outside the scope of this Inquiry. Federal legislation governing the interception of telecommunications, however, contains provisions about the use, disclosure and storage of information which also may be 'personal information'. These provisions,

---

7 Ibid, [1.8.1].

8 *Telecommunications (Interception and Access) Act 1979* (Cth) ch 3.

9 See, eg, Ibid ss 9(1)(a), 46(1)(d). S Bronitt, J Stellios and K Leong, *Submission PR 213*, 27 February 2007. See also S Bronitt and J Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' (2006) 24 *Prometheus* 414.

10 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, 6.

11 Ibid, rec i.

12 These provisions are discussed in detail in Chs 71 and 72.

and their interaction with the *Privacy Act*, are within the scope of the Inquiry and are discussed further below.

Telecommunications (Interception and Access) Act

Interception and stored communications

73.9 The *Telecommunications (Interception and Access) Act* makes it an offence to intercept a communication passing over a telecommunications system without the knowledge of the maker of the communication, or to access a 'stored communication'[13] without the knowledge of the sender or intended recipient of the communication.[14] There are exceptions to these general offence provisions. Most importantly, law enforcement agencies can intercept or access communications if they have obtained a warrant to do so. In addition, other individuals, such as employees of telecommunication providers, can intercept or access communications in limited circumstances.[15]

73.10 The *Telecommunications (Interception and Access) Act* provides for two communication interception warrant processes. Part 2.2 of the Act provides for the issuing of warrants authorising the Australian Security Intelligence Organisation (ASIO) to intercept telecommunications (ASIO warrants). ASIO warrants are issued by the Attorney-General at the request of the Director-General of Security.[16] Part 2.5 sets out a process for the issuing of warrants to agencies other than ASIO to intercept telecommunications. These agencies include Australian Government and state agencies, including a state police force and other bodies such as the Queensland Crime and Misconduct Commission.[17] These warrants (agency warrants) are issued by a judge or a nominated member of the Administrative Appeals Tribunal (AAT).[18]

73.11 The Act also sets out a warrant process for access to stored communications.[19] Whereas the interception warrant regime is limited to law enforcement agencies, applications for stored communication warrants can be made by all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This includes the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission.[20] Warrants are issued by an 'issuing authority' appointed by the Attorney-General and may include judges of courts exercising federal jurisdiction, a Federal Magistrate, or a magistrate. The Attorney-General also may appoint AAT members who are legal practitioners of at least 5 years standing.[21]

---

13 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 6, 7.
14 Ibid s 108.
15 See, eg, Ibid ss 7(2)(a), 108(2)(d).
16 Ibid s 9.
17 Ibid s 34.
18 Ibid s 46.
19 Ibid pt 3.
20 Ibid s 110; *Telecommunications Act 1997* (Cth) s 282.
21 *Telecommunications (Interception and Access) Act 1979* (Cth) s 6DB.

73.12 The *Telecommunications (Interception and Access) Act* makes it an offence to record, use or disclose intercepted information, stored communication information, or information about an interception or stored communication warrant, except in certain circumstances.[22] For example, this type of information can be recorded, used or disclosed for the purpose of applying for a warrant or for investigating certain offences.[23]

73.13 The Act also contains a requirement that records of intercepted or stored communications be destroyed in certain circumstances.[24] Law enforcement agencies are obliged to keep records relating to interception and stored communication warrants,[25] and to provide the responsible Minister (currently the Attorney-General)[26] with an annual report containing information about these warrants.[27] The Minister is required to compile information received from law enforcement agencies into a report that must be tabled in Parliament.[28] Civil remedies also are available for unlawful interception of communications.[29]

Telecommunications data

73.14 Chapter 4 of the *Telecommunications (Interception and Access) Act* sets out when the offence provisions under ss 276, 277 and 278 of the *Telecommunications Act* do not prohibit the disclosing of information or documents ('telecommunications data') to ASIO and enforcement agencies by certain participants in the telecommunications industry (referred to in this chapter as 'telecommunications service providers').[30] 'Telecommunications data' is not defined under the Act.[31]

73.15 The Chapter sets out a two-tier access regime for 'historical telecommunications data' and 'prospective telecommunications data'. Under s 176(2) of the Act, certain ASIO staff can authorise telecommunications service providers to disclose information or documents that come into existence during the period for which the authorisation is in force (prospective telecommunications data). These persons also may authorise the disclosure of information or documents that existed before the time the authorisation came into force (historical telecommunications data).[32]

73.16 The level of authorisation required for access to prospective telecommunications data is higher than that required for historical telecommunications data. Under s 175(2)

---

22 Ibid pt 2.6, pt 3.4 div 2.
23 Ibid ss 63AA, 71, 134, 140.
24 Ibid ss 79 and 150. See discussion below.
25 Ibid pts 2.7, 3.5.
26 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008, sch pt 2.
27 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.8 div 1, pt 3.6 div 1.
28 Ibid pt 2.8 div 2, pt 3.6 div 2.
29 Ibid pts 2.10, 3.7.
30 These provisions are discussed in detail in Chs 71 and 72.
31 *Telecommunications (Interception and Access) Act 1979* (Cth) s 172. See discussion of the meaning of 'telecommunications data' below.
32 Ibid s 176(3).

and (4), the Director-General of ASIO could allow any officer or employee of ASIO to authorise access to historical telecommunications data, whereas in the case of prospective telecommunications data, authorisation is limited to Senior Executive Service (SES) Band 2 or above.[33] The authorisation commences at the time the person from whom the disclosure is sought receives notification of the authorisation, and must end within 90 days, unless revoked earlier.[34]

73.17 Sections 178 and 179 allow an authorised officer of an 'enforcement agency' to authorise a telecommunications service provider to disclose historical data if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law, or a law imposing a pecuniary penalty or protection of the public revenue. 'Enforcement agencies' include: 'criminal law enforcement agencies' (for example, the Australian Federal Police and state and territory police); the CrimTrac Agency; and any body whose functions include administering a law imposing a pecuniary penalty or relating to the protection of the public revenue.[35]

73.18 Section 180 allows an authorised officer of a 'criminal law-enforcement agency' to authorise the disclosure of prospective telecommunications data. In making the authorisation, the officer must be satisfied that the disclosure is reasonably necessary for the investigation of a Commonwealth, state or territory offence that is punishable by imprisonment for at least three years. The officer also must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.[36] The authorisation period is half that allowed for ASIO investigations—45 days. [37]

Interaction with the *Privacy Act*

73.19 It is possible that information intercepted or accessed under the *Telecommunications (Interception and Access) Act* could constitute 'personal information' for the purposes of the *Privacy Act.* Accordingly, the handling of information under the *Telecommunications (Interception and Access) Act* also could be regulated under the *Privacy Act.*

73.20 The acts and practices of ASIO are completely exempt from the requirements of the *Privacy Act*.[38] Consequently, the handling of personal information that has been intercepted or accessed by ASIO will be regulated under the *Telecommunications (Interception and Access) Act* and guidelines issued by the Attorney-General under the *Australian Security Intelligence Organisation Act 1979* (Cth).[39]

---

33 The Senior Executive Service (SES) constitutes the senior management and leadership group of the Australian Public Service.

34 *Telecommunications (Interception and Access) Act 1979* (Cth) s 176(5).

35 Ibid s 5.

36 Ibid s 180(5).

37 Ibid s 180(6).

38 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2)(a). See Ch 34.

39 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 21 May 2008. See discussion in Ch 34.

73.21 Most Australian Government law enforcement agencies, such as the Australian Federal Police, are subject to the Information Privacy Principles (IPPs) under the *Privacy Act*.[40] The acts and practices of these agencies in relation to the handling of personal information, therefore, are regulated by the *Telecommunications (Interception and Access) Act* and the *Privacy Act.*

73.22 The handling of personal information in accordance with the *Telecommunications (Interception and Access) Act* generally will fall within an exception to one of the IPPs, and therefore comply with the *Privacy Act*. For example, the use and disclosure of personal information pursuant to the *Telecommunications (Interception and Access) Act* will be a use or disclosure that is 'required or authorised by or under law' under IPP 10 and IPP 11—and the 'Use and Disclosure' principle under the model Unified Privacy Principles (UPPs).[41] If a law enforcement agency engages in an act or practice that does not comply with the *Telecommunications (Interception and Access) Act*, the act or practice would not be 'authorised by or under law' and so may breach the privacy principles.

73.23 Similarly, a telecommunications service provider that discloses personal information to ASIO or a law enforcement agency in a way that is authorised under the *Telecommunications (Interception and Access) Act* will not be in breach of National Privacy Principle (NPP) 2. An act or practice engaged in pursuant to any of the exceptions under the *Telecommunications (Interception and Access) Act* is an act or practice that is 'authorised by or under law' for the purposes of NPP 2.[42]

Communications and 'telecommunications data'

73.24 The *Telecommunications (Interception and Access) Act* regulates 'communications', 'stored communications' and 'telecommunications data'. As noted above, it is possible that this information could constitute 'personal information' for the purposes of the *Privacy Act.*

73.25 The *Telecommunications (Interception and Access) Act* defines 'communications' as including a conversation and a message, and any part of a conversation or message, whether in the form of: speech, music or other sounds; data; text; visual images, whether or not animated; signals or in any other form or in any combination of forms.[43] A 'stored communication' is defined as a communication that: is not passing over a telecommunications system; is held on equipment that is operated by, and is in the possession of, a carrier; and cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

---

40 See discussion in Ch 37.
41 See Ch 25.
42 See Chs 25 and 71.
43 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

73.26 Chapter 4 of the *Telecommunications (Interception and Access) Act* regulates access to 'telecommunications data', but does not set out a definition of 'telecommunications data'. Chapter 4, like the exceptions under Part 13 of the *Telecommunications Act*, authorise access to 'information or a document'.[44] 'Telecommunications data', therefore, would be either information or a document.

73.27 The Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007 that introduced Chapter 4 provides that:

> Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.
>
> For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session and the start and finish time of each session.[45]

73.28 Submissions to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 raised concerns about the meaning of 'telecommunications data'.[46]

73.29 In DP 72, the ALRC noted that in light of the recent Senate Committee Inquiry, it did not propose to conduct another detailed study of the Telecommunications (Interception and Access) Amendment Bill 2007. The ALRC noted, however, that it shared a number of the concerns raised in submissions to the Senate Committee Inquiry. The ALRC asked whether the Telecommunications (Interception and Access) Amendment Bill 2007 (as it was then known) should be amended to define 'telecommunications data'.[47]

Submissions and consultations

73.30 A number of stakeholders supported amending the *Telecommunications (Interception and Access) Act* to define 'telecommunications data'.[48] For example, the Office of the Victorian Privacy Commissioner (OVPC) submitted that the term should be defined to at least clarify whether specific technologies are included in the term.[49]

---

44 See, eg, Ibid s 175. The information regulated under Part 13 is discussed in detail in Ch 71.

45 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), 6.

46 Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), [3.11]–[3.16]. See also Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), Minority Report by the Australian Democrats.

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–2(a).

48 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

49 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

73.31 The Law Council of Australia noted the definition in the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007 that 'telecommunications data' is 'information about a telecommunications, but does not include the contents or substance of the communication'. The Law Council submitted that this definition is workable to the extent that there is a distinction between the 'contents or substance' of a communication, and all other information about the communication. The Law Council suggested, however, that such a distinction cannot be drawn. The Law Council submitted that it is important to set out in positive terms exactly what type of personal information falls within the meaning of 'telecommunications data'.[50]

73.32 Other stakeholders did not support defining 'telecommunications data'. The Attorney-General's Department (AGD) submitted that the exclusion of an exhaustive definition for telecommunications data is consistent with the technology-neutral language of the *Telecommunications (Interception and Access) Act*. The AGD also noted that it provides guidance to agencies and carriers regarding these issues, both generally and on a case-by-case basis.[51]

ALRC's view

73.33 The ALRC does not recommend amending the *Telecommunications (Interception and Access) Act* to define 'telecommunications data'. The exclusion of a definition enables the legislation to remain technology neutral so that it can be applied to new developments in technology without the need for amendment. This approach is consistent with the technology-neutral approach of the *Privacy Act*,[52] and Part 13 of the *Telecommunications Act*.

73.34 There should be more guidance, however, about what is meant by 'telecommunications data'. Provision of this information to ASIO and enforcement agencies is a significant invasion of privacy. Telecommunications data allows agencies to monitor when, how and with whom an individual communicates; what websites they access; and, in the case of mobile phones, an individual's location. Intelligence and law enforcement agencies, telecommunications service providers, regulators, other oversight bodies (such as the Inspector-General of Intelligence and Security (IGIS)), and the community should have a clear understanding, therefore, about what information may be disclosed under these laws.

73.35 Below the ALRC recommends that the AGD should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act*. This guidance should address what the term 'telecommunications data' means in various contexts.[53]

---

50 Law Council of Australia, *Submission PR 527*, 21 December 2007.
51 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
52 See Ch 10.
53 Rec 73–5.

Collection

73.36 The interception of, or access to, personal information by a law enforcement agency under the *Telecommunications (Interception and Access) Act* complies with IPP 1 where the collection is 'lawful' and 'necessary for one or more of its functions or activities'. This also would be the case of the 'Collection' principle under the model UPPs.[54]

Stored communications

73.37 The *Telecommunications (Interception) Amendment Act* expanded the circumstances under which stored communications can be accessed to allow 'warrantless' access to stored communications. The *Telecommunications (Interception and Access) Act* allows for stored communications to be accessed without a warrant where one party to that communication has knowledge of the access.[55] A party has 'knowledge' where he or she has been provided with written notice.[56]

73.38 Professor Simon Bronitt, James Stellios and Kevin Leong submitted that this provision creates a regulatory loophole—officials are not required to obtain a warrant to access stored communications in cases where notification is given to one of the parties to a stored communication. It was argued that further consideration must be given to the significance and scope of notification, with careful evaluation of the reasonable expectations of privacy in relation to stored communications and the competing public interests.[57]

73.39 The fact that this provision allows for the invasion of privacy of many individuals, including non-suspect persons, is of concern. For example, a communication involving multiple participants (including non-suspects), such as an online bulletin board, could be accessed if one participant in that communication was given written notice of the access. As noted above, however, it is the ALRC's view that the circumstances in which communications can be intercepted is an issue that is outside the scope of this Inquiry. This issue should be considered as part of the review of telecommunications legislation recommended in Chapter 71.[58]

Telecommunications data

73.40 Under s 180 of the *Telecommunications (Interception and Access) Act*, an authorised officer of a 'criminal law enforcement agency' must not make an authorisation to access prospective telecommunications data unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of an offence against a law of the Commonwealth, a state or a territory that is punishable by imprisonment for at least three years. Section 180(5) of the *Telecommunications*

---

54 See Ch 21.
55 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(1)(b).
56 Ibid s 108(1A).
57 S Bronitt, J Stellios and K Leong, *Submission PR 213*, 27 February 2007. See also I Graham, *Submission PR 427*, 9 December 2007.
58 Rec 71–2.

(Interception and Access) Act provides that, before making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.[59]

73.41 Submissions to the Senate Committee Inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 suggested that greater guidance was needed on how the privacy implications of an authorisation should be considered and documented under s 180(5).[60] In DP 72, the ALRC asked whether the Telecommunications (Interception and Access) Amendment Bill 2007 (as it was then known) should be amended to provide greater guidance in this regard.[61]

Submissions and consultations

73.42 A number of stakeholders supported the amendment of the legislation to provide greater guidance on how the privacy implications of an authorisation should be considered and documented.[62]

73.43 The Law Council of Australia submitted that the requirement to 'have regard to' a person's privacy under s 180(5) is likely to receive little more than 'lip service', based on experience with the *Surveillance Devices Act 2004* (Cth), which contains a similar provision.[63] The Law Council submitted that s 180(5) should be amended to express in clear terms the test to be applied. The Law Council suggested the following formulation:

> Before making the authorisation, the appropriate authorising officer must be satisfied on reasonable grounds that the likely benefit to the criminal investigation which will result from the disclosure substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons.[64]

73.44 Other stakeholders did not agree that further guidance was needed.[65] The AGD noted that s 183 provides that an authorisation must comply with the requirements determined by the Communications Access Co-ordinator, who must consult with the Privacy Commissioner before making such a determination. The AGD submitted that the initial determination to be made under this section will include guidance to agencies on how to determine the impact on privacy.[66]

---

59 *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(4)–(5).

60 Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), [3.34]–[3.37].

61 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–2(b).

62 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Police Federation of Australia, *Submission PR 385*, 6 December 2007.

63 *Surveillance Devices Act 2004* (Cth) s 16(2)(c).

64 Law Council of Australia, *Submission PR 527*, 21 December 2007.

65 Australian Federal Police, *Submission PR 545*, 24 December 2007.

66 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

ALRC's view

73.45 Greater guidance should be provided about how the privacy implications of an authorisation are to be considered and documented under s 180(5) of the *Telecommunications (Interception and Access) Act*. The ALRC notes that a determination is to be made under s 183 of the *Telecommunications (Interception and Access) Act* that will address this issue. The determination should ensure that the issue of privacy is addressed directly and transparently in the authorisation process. This will avoid the situation where an authorising officer could just 'tick a box' to indicate that he or she has considered privacy issues.

Use and disclosure

73.46 The *Telecommunications (Interception and Access) Act* makes it an offence to record, use or disclose intercepted information, stored communication information, or information about an interception or stored communication warrant, except in certain circumstances.[67] As noted above, the use and disclosure of personal information by an agency pursuant to the *Telecommunications (Interception and Access) Act* is a use or disclosure that is 'required or authorised by or under law' under IPPs 10 and 11. Further, a telecommunications service provider that discloses personal information to ASIO or a law enforcement agency in a way that is authorised under the *Telecommunications (Interception and Access) Act* will not be in breach of NPP 2.[68]

Performance of person's duties

73.47 Under ss 63B(1) and 135(3) of the *Telecommunications (Interception and Access) Act*, an employee of a carrier may communicate or make use of lawfully intercepted or accessed information or information that has been obtained by accessing a stored communication in the performance of his or her duties.[69] In DP 72, the ALRC noted that the scope of the exceptions under ss 63B(1) and 135(3) is unclear. The ALRC asked whether the provisions should be amended to clarify when an employee of a carrier may communicate or make use of lawfully intercepted or accessed information in the performance of his or her duties.[70]

Submissions and consultations

73.48 The Office of the Privacy Commissioner (OPC) submitted that ss 63B(1) and 135(3) should be aligned with the 'Use and Disclosure' principle so that the use or disclosure of personal information for a purpose other than the primary purpose of collection (the secondary purpose) would be permitted if:

---

67 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.6, pt 3.4 div 2.

68 See Ch 25.

69 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 63B(1), 135(3). Sections 279 and 296 of the *Telecommunications Act* provide for a similar exception in relation to the performance of a person's duties as an employee or contractor of a telecommunications service provider. These provisions are discussed in detail in Ch 72.

70 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 64–1.

- the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
- the individual would reasonably expect the agency or organisation to use or disclose the information for a secondary purpose.[71]

73.49 One stakeholder submitted that ss 63B(1) and 135(3) should be amended to confine its scope to where disclosure is necessary to permit an intercepted or accessed communication to be transmitted to the intended recipient of the communication.[72]

73.50 Telstra submitted that ss 63B and 135 should not be confined, as they are necessary for the supply of a number of telecommunications services.[73] Telstra also submitted that the provisions should be amended to cover contractors of a carrier as well as employees, because in reality many functions of a carrier are performed by contractors.[74]

ALRC's view

73.51 The ALRC does not make any recommendation to modify the scope of ss 63B(1) and 135(3) of the *Telecommunications (Interception and Access) Act*. The ALRC considered confining the scope of the provisions to certain duties of an employee or contractor. In the ALRC's view, however, this option would be unworkable in a complex and changing telecommunications environment. The ALRC also considered aligning the exception with the 'Use and Disclosure' principle under the model UPPs. The ALRC is concerned, however, that confining the scope of the exception in this way may have unforeseen consequences and accepts Telstra's view that it may prevent the provision of telecommunications services.

73.52 The ALRC sees merit in amending the exceptions under ss 63B and 135 of the Act to cover contractors of a carrier as well as employees. In the ALRC's view, this issue requires further consultation and should be considered in the review of telecommunications legislation recommended in Chapter 71.[75]

Business needs of other carriers or service providers

73.53 Under ss 63B(2) and 135(4) of the *Telecommunications (Interception and Access) Act*, intercepted and accessed information may be communicated to another carrier (which may include a carriage service provider)[76] if:

---

71 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
72 I Graham, *Submission PR 427*, 9 December 2007.
73 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See also Optus, *Submission PR 532*, 21 December 2007.
74 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
75 Rec 71–2.
76 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

- the communication of the information is for the purpose of the carrying on by the other carrier of its business relating to the supply of services by means of a telecommunications network; and
- the information relates to the supply of services by the other carrier by means of a telecommunications network.

73.54 Sections 291 and 302 of the *Telecommunications Act* provide for a similar exception in relation to the use and disclosure of information or documents obtained during the supply of telecommunications services.[77]

73.55 The Australian Communications and Media Authority (ACMA) has noted that s 135(4) of the *Telecommunications (Interception and Access) Act* is significantly broader than s 291 of the *Telecommunications Act*.[78] In ACMA's view, s 135(4) may be used by carriers and carriage service providers to disclose to each other personal information in stored communications that could not have been disclosed under the *Telecommunications Act*. In DP 72, the ALRC asked how ss 63B(2) and 135(4) of the *Telecommunications (Interception and Access) Act*) should be clarified.[79]

Submissions and consultations

73.56 One stakeholder submitted that ss 63B(2) and 135(4) should be amended to limit disclosure to when it is necessary to enable an intercepted or accessed communication to be transmitted to the intended recipient of the communication.[80]

73.57 The OPC argued that ss 63B(2) and 135(4) should be aligned with the 'Use and Disclosure' principle so that the use or disclosure of personal information for a purpose other than the primary purpose of collection (the secondary purpose) would be permitted if:

- the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
- the individual would reasonably expect the agency or organisation to use or disclose the information for a secondary purpose.[81]

73.58 The AGD submitted that ss 63B(2) and 135(4) were introduced to enable information to be used or communicated between telecommunications service providers that are operating on the same network to enable the communication of information from products that travel over different networks. The AGD's

---

77 These provisions are discussed in detail in Ch 72.
78 Section 291 of the *Telecommunications Act 1997* (Cth) is discussed in Ch 71.
79 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 64–2.
80 I Graham, *Submission PR 427*, 9 December 2007.
81 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

understanding is that these are the only purposes for which these provisions are utilised.[82]

73.59 Telstra submitted that the provisions should not be confined as they are necessary for a number of purposes, including the supply of services such as spam filtering and virus checking to customers, and for fault diagnosis and rectification of reported faults.[83]

ALRC's view

73.60 The ALRC does not make any recommendation to modify the scope of ss 63B(2) and 135(4) of the *Telecommunications (Interception and Access) Act*. The ALRC considered aligning these provisions with the 'Use and Disclosure' principle under the model UPPs. The ALRC also considered confining these provisions to permit an employee of a carrier to communicate to another carrier intercepted or accessed information in the same circumstances as permitted under s 291 of the *Telecommunications Act*. The ALRC is concerned, however, about any unforeseen consequences of such amendments, including the prevention of the seamless interconnection between carriers and carriage service providers.

B-Party warrants

73.61 The Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006 heard a substantial number of concerns relating to the interception of B-Party communications.[84] The Committee noted that a principal problem with the B-Party warrant is the potential for collecting a great deal of information which may be incidental to, or not associated with, the investigation for which the warrant was issued.

> As Senator Ludwig noted, 'it is not only the B-Party but also the C, D E and F parties who may at some point end up talking to B and, therefore, being captured'. The result is that potentially not just one, but a great many non-suspects to be caught in the B-Party warrant process.[85]

73.62 The Committee recommended that the Bill be amended to:

- provide that certain material obtained under a B-Party warrant will be exempted from use under the legislation, including communications between solicitor and client; clergy and devotee; doctor and patient; and communications by the

---

82 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007. See also Law Council of Australia, *Submission PR 527*, 21 December 2007.

83 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See also Optus, *Submission PR 532*, 21 December 2007. In the ALRC's view, the provisions are not required for fault diagnosis and rectification. Use and disclosure for these purposes is permitted under *Telecommunications (Interception and Access) Act 1979* (Cth) ss 7 and 108.

84 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), ch 4.

85 Ibid, [4.62].

innocent person with any person other than the person of interest to the law enforcement agency; and

- introduce defined limits on the use and derivative use of material collected by a B-Party warrant.[86]

73.63 The Australian Government did not accept these recommendations. It considered that it is impractical and inappropriate to require an assessment of whether communications may attract legal professional privilege.[87] The Government also noted that material collected by a B-Party warrant is subject to the same rules as other warrants under Part 2.6 of the *Telecommunications (Interception and Access) Act*, and that the derivative use of information is restricted to circumstances where the intercepted information appears to relate to the commission of a serious offence which should be investigated by another agency.[88] Further, the communication of intercepted information by intercepting agencies is subject to the oversight of the Commonwealth Ombudsman and state equivalents.[89]

73.64 In DP 72, the ALRC noted with concern the potential to collect large amounts of information about non-suspect persons under B-Party warrants compared with other types of warrants. The ALRC asked whether further restrictions should apply to the use and disclosure of information obtained under a B-Party interception warrant under the *Telecommunications (Interception and Access) Act.*[90]

Submissions and consultations

73.65 The OPC submitted that there should be tighter restrictions on the use and disclosure of material collected under a B-Party warrant, including prohibitions on the use or disclosure of intercepted material for any purpose other than the purpose stated in the warrant. It submitted also that there should be enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant should be destroyed immediately.[91]

73.66 The Law Council of Australia submitted that innocent third parties should not be subject to covert surveillance and recommended that the provisions relating to B-Party warrants be repealed. The Law Council submitted, however, that under the current arrangements:

---

86 Ibid, rec 23.

87 Australian Government Attorney-General's Department, Government Response to the Senate Legal and Constitutional Legislation Committee Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006 (2006), 10.

88 *Telecommunications (Interception and Access) Act 1979* (Cth) s 68.

89 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional Legislation Committee Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), 11.

90 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 64–3.

91 The OPC submitted that prohibitions on the use or disclosure of intercepted material should be subject to an exception in relation to the investigation of serious criminal offences: Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

> Except in cases of emergency or imminent threat, there should be a clear prohibition on the use or disclosure of any information derived from intercepting a communication between the B-Party and a person other than the suspect. Although such a prohibition may deny agencies the benefits of valuable information unexpectedly obtained using a B-Party warrant, it is a necessary safeguard against the misuse of personal information.[92]

73.67 The Law Council also recommended that the *Telecommunications (Interception and Access) Act* should impose strict procedures for identifying and protecting otherwise privileged communications which may be obtained—for example, by intercepting communications between doctor and patient and a lawyer and client.[93]

73.68 Other stakeholders submitted that the provisions regulating the use and disclosure of information obtained under a B-Party warrants were sufficient.[94] The AGD submitted that there are currently stringent controls on the use and disclosure of intercepted information under the *Telecommunications (Interception and Access) Act*, and that these controls apply equally to all interception warrants, including B-Party warrants.[95]

ALRC's view

73.69 The ALRC is concerned about the potential to collect, use and disclose a large amount of information about non-suspect persons under a B-Party warrant compared with other types of warrants. The ALRC, however, does not make a recommendation to restrict further the use and disclosure of information obtained under a B-Party interception warrant. The ALRC is concerned that any further restriction on the use and disclosure of this information may compromise the investigation of unlawful activities and hinder effective law enforcement. This issue should be the subject of further consultation, and should be considered as part of the review of telecommunications legislation recommended in Chapter 71.[96]

Secondary use and disclosure of telecommunications data

73.70 Section 182(1) of the *Telecommunications (Interception and Access) Act* provides that it is an offence if telecommunications data are disclosed to an enforcement agency and that agency uses or discloses those data. There is no general

---

92 Law Council of Australia, *Submission PR 527*, 21 December 2007.

93 Ibid. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; I Graham, *Submission PR 427*, 9 December 2007.

94 Australian Federal Police, *Submission PR 545*, 24 December 2007; Confidential, *Submission PR 488*, 19 December 2007.

95 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

96 See Rec 71–2. The Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006 recommended that the legislation introducing the B-Party warrant should be reviewed within five years: Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), rec 25.

prohibition on the secondary use or disclosure of telecommunications data by ASIO. The prohibition under s 182(1) does not apply if:

- the disclosure is reasonably necessary for the performance by ASIO of its functions, for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue (s 182(2)); or
- the use is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue (s 182(3)).

Submissions and consultations

73.71 The Law Council of Australia submitted that the secondary use and disclosure should not allow a law enforcement agency to disclose information obtained under an authorisation:

- to an agency which is not itself able to authorise and access prospective telecommunications data; or
- for a purpose which is not itself capable of providing grounds for an authorisation to access prospective telecommunications data.[97]

73.72 The Law Council of Australia also submitted that the general prohibition in s 182(1) should also apply to telecommunications data obtained by ASIO.[98]

ALRC's view

73.73 The ALRC is concerned about the breadth of s 182(2) and (3) of the *Telecommunications (Interception and Access) Act*. The ALRC also is concerned, however, that a recommendation to confine the scope of these provisions could compromise the investigation of unlawful activities and hinder effective law enforcement. The IGIS and the Commonwealth Ombudsman should monitor the secondary use and disclosure of telecommunications data under s 182(2) and (3). These provisions also should be considered as part of the review recommended in Chapter 71.[99]

73.74 The ALRC notes that the prohibition on secondary use or disclosure of telecommunications data under s 182 of the *Telecommunications (Interception and Access) Act* does not cover information that has been disclosed to ASIO. It is unnecessary to extend these provisions to ASIO because ASIO officers, employees and contractors are subject to strict secrecy provisions.

73.75 For example, s 18 of the *Australian Security Intelligence Organisation Act 1979* (Cth) provides that it is an offence for a person to communicate information that has come to the knowledge or into the possession of the person by reason of his or her being an officer, employee or contractor of ASIO. Section 18(3) sets out the

---

97 Law Council of Australia, *Submission PR 527*, 21 December 2007.
98 Ibid.
99 Rec 71–2.

circumstances in which disclosure of this information is permitted—for example, information may be disclosed to a state or territory police officer if the information relates to the intended commission of an indictable offence.

Voluntary disclosure of telecommunications data

73.76 Chapter 4 of the *Telecommunications (Interception and Access) Act* sets out when an employee of a telecommunications service provider can 'voluntarily disclose' telecommunications data (that is, in the absence of formal disclosure authorisation from an enforcement agency). Chapter 4 provides that a telecommunications service provider may voluntarily disclose telecommunications data to:

- ASIO, if the disclosure is in connection with the performance by ASIO of its functions (s 174); and
- an enforcement agency, if the disclosure is reasonably necessary for the enforcement of the criminal law (s 177(1)); or a law imposing a pecuniary penalty; or for the protection of the public revenue (s 177(2)).

Submissions and consultations

73.77 The Law Council of Australia submitted that the voluntary disclosure provisions, particularly s 174, require amendment. The Law Council submitted that s 174 should set out explicitly the circumstances in which voluntary disclosure of telecommunications data to ASIO is permitted. The Law Council submitted that articulating in more detail the threshold test for voluntary disclosure may reduce the risk that personal information will be disclosed to ASIO for an unauthorised purpose.[100]

ALRC's view

73.78 Employees of telecommunications service providers require further guidance about when they may disclose voluntarily telecommunications data to ASIO and enforcement agencies. There is a risk that without further guidance, the voluntary disclosure provisions in the *Telecommunications (Interception and Access) Act* could result in the inappropriate disclosure of telecommunications data. Employees of telecommunications service providers do not have expertise in determining when disclosure of telecommunications data is 'reasonably necessary' for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

73.79 The ALRC recommends below that the AGD should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act.* This guidance should address the

100 Law Council of Australia, *Submission PR 527,* 21 December 2007.

circumstances in which voluntary disclosure of telecommunications data to ASIO and other enforcement agencies is permitted.[101]

Retention and destruction of records

Intercepted material

73.80 Section 79 of the *Telecommunications (Interception and Access) Act* provides that a record, 'other than a copy', obtained by means of an interception must be destroyed if the chief officer of an agency is satisfied that it is unlikely that it will be required for certain permitted purposes. The Blunn Report noted that it was 'curious' that the requirement to destroy a record under s 79 did not extend to copies of the record.[102] Section 150 of the Act contains a similar requirement to destroy information or a record obtained by accessing a stored communication. This section, introduced in 2006, does not distinguish between a record and a copy of a record.[103]

73.81 In DP 72, the ALRC expressed the view that the same destruction rules should apply to records and copies of records. The ALRC proposed that s 79 of the *Telecommunications (Interception and Access) Act* should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.[104]

Submissions and consultations

73.82 A number of stakeholders supported the proposal.[105] Others, however, opposed the proposal.[106] For example, the AGD submitted that the requirement to destroy copies was excluded from s 79 because of enforcement issues. For example, agencies could not enforce destruction of copies given to other agencies for permitted purposes, or where the information appeared on the public record. The AGD also noted that copies of lawfully intercepted information may be made only in limited circumstances under the *Telecommunications (Interception and Access) Act*, and that any copies of the information continued to be protected from further use or communication.[107]

73.83 One stakeholder submitted that lawfully intercepted information is often included in operational documents, and that it would be impossible to comply with a requirement that these types of documents be destroyed because they include copies of intercepted material. The stakeholder also submitted that the proposal could create an

---

101 See Recommendation 73–5.

102 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, [9.4].

103 Section 150 is discussed below.

104 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–1

105 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Law Council of Australia, *Submission PR 527*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

106 Australian Federal Police, *Submission PR 545*, 24 December 2007.

107 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007. See also Confidential, *Submission PR 488*, 19 December 2007.

unjustified administrative burden on interception agencies. A requirement to destroy all copies would mean that very stringent record-keeping measures would need to be in place to ensure that the whereabouts of every copy was logged.[108]

ALRC's view

73.84 The ALRC recommends that s 79 of the *Telecommunications (Interception and Access) Act* be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose. The ALRC can see no reason why copies of information obtained from a stored communication warrant are required to be destroyed, but that copies of information obtained from an interception warrant are not.

73.85 The covert nature of interception and access to communications requires the safeguard that the intercepted or accessed information is destroyed as soon as it is no longer required. The 'Data Security' principle under the UPPs provides that an agency or organisation must destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.[109] This rule should apply to records as well as copies of records of intercepted information. Agencies should not be able to retain copies of records indefinitely.

Recommendation 73–1 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, in the possession of an agency, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

Stored communications

73.86 In its submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006, the OPC suggested that s 150 may result in it being 'lawful for an agency to keep irrelevant information indefinitely'.[110]

73.87 The Senate Legal and Constitutional Affairs Committee recommended that the Bill be amended to specify time limits within which an agency must review their holdings of information accessed via a stored communications warrant and destroy

108 Confidential, *Submission PR 488*, 19 December 2007.

109 See discussion in Ch 28.

110 Office of the Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006.

information as required under the proposed s 150. The Committee stated its view that, given the potential to collect vast amounts of irrelevant information under a stored communications warrant, such a safeguard was essential.[111]

73.88 The Australian Government did not accept this recommendation. It noted that the current requirements under s 150 are sufficient and that the Commonwealth Ombudsman is required to inspect an agency's records to ascertain compliance with the destruction of records and report to the Attorney-General. Additionally, agencies are required to provide a report to the Attorney-General that sets out the extent to which records are destroyed.[112]

73.89 In its submission to the current Inquiry, the OPC reiterated its concerns about s 150, noting that it appeared that, until the chief officer has considered the relevant matters, the agency lawfully may keep the information or record. Without greater specificity, the OPC is concerned that in some circumstances it may be lawful for an agency to keep irrelevant information indefinitely.[113]

73.90 The ALRC does not recommend the amendment of s 150 to specify when information obtained by a stored communication warrant should be destroyed. There is a need for greater guidance, however, about when information should be destroyed under the provision. Below the ALRC recommends that the AGD should provide guidance on when the chief officer of an agency must cause information to be destroyed when it is no longer needed for a permitted purpose under s 150 of the *Telecommunications (Interception and Access) Act*.

Destruction of non-material content

73.91 The retention and destruction of information obtained by B-Party warrants will be subject to s 79 of the *Telecommunications (Interception and Access) Act*. In its submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006, the OPC expressed concern about the absence of rules to require the destruction of material outside the scope of the purpose stated in a B-Party warrant. It recommended 'enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed'.[114]

73.92 The Senate Legal and Constitutional Affairs Committee recommended that there should be strict supervision arrangements introduced to ensure the destruction of non-

111 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [3.79]–[3.80], rec 10.

112 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional Legislation Committee Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), 5.

113 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

114 Office of the Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006.

material content.[115] The Australian Government did not accept this recommendation. It stated that the current rules under the *Telecommunications (Interception and Access) Act* relating to the destruction of information obtained by a warrant under Part 2.6 already require the destruction of this material.[116]

73.93 In DP 72, the ALRC expressed concerns about the large amount of information that can be obtained under a B-Party warrant and proposed that s 79 of the *Telecommunications (Interception and Access) Act* be amended to require expressly the destruction of non-material content intercepted under a B-Party warrant.[117]

Submissions and consultations

73.94 A number of stakeholders supported the proposal.[118] The Law Council of Australia submitted that any express requirement to destroy non-material content must be accompanied by guidance as to what constitutes 'material information'. In the Law Council's view, whether information is 'material' should be determined by reference to the grounds advanced to justify the issuance of the B-Party warrant.[119]

73.95 Other stakeholders opposed the proposal.[120] The AGD submitted that s 79 already requires the destruction of information not likely to be required for a permitted purpose.[121] One stakeholder noted that there is an inherent danger in selectively deleting material. For instance, a defendant may claim that material that was deleted for being non-material had exculpatory value.[122]

ALRC's view

73.96 The ALRC is concerned that a large amount of information can be obtained about non-suspects under a B-Party warrant, and that copies of records are not currently required to be destroyed under s 79. It is arguable that s 79 already requires the destruction of information that is outside the scope of the permitted purposes of a B-Party warrant. In the interest of clarity, however, the ALRC recommends that s 79 of

---

115 Office of the Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006, rec 24.

116 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional Legislation Committee Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), 11.

117 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–3.

118 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

119 The Law Council noted that the only qualification that it would place on the provision of guidance is that any destruction regime must be careful not to compromise record-keeping obligations that are designed to ensure proper scrutiny of the exercise of covert information-gathering powers: Law Council of Australia, *Submission PR 527*, 21 December 2007.

120 Australian Federal Police, *Submission PR 545*, 24 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

121 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

122 Confidential, *Submission PR 488*, 19 December 2007.

the *Telecommunications (Interception and Access) Act* be amended to require expressly the destruction of non-material content intercepted under a B-Party warrant.

73.97 The ALRC recommends below that the AGD should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act.* This guidance should address the destruction of non-material content.

> **Recommendation 73–2** Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to require the destruction of non-material content intercepted under a B-Party warrant.

Telecommunications data

73.98 There are no provisions under the *Telecommunications (Interception and Access) Act* that require ASIO or law enforcement agencies to destroy telecommunications data when it is no longer required for a permitted purpose. While the retention of this information by law enforcement agencies may be regulated by the *Privacy Act*, the acts and practices of ASIO are exempt from the requirements of the *Privacy Act*.[123] Further, the guidelines issued by the Attorney-General under the *Australian Security Intelligence Organisation Act* are silent on the destruction of information.[124]

73.99 In DP 72, the ALRC asked whether the Telecommunications (Interception and Access) Amendment Bill 2007 (as it was then known) should be amended to include positive obligations on law enforcement agencies to destroy in a timely manner irrelevant material containing personal information and information which is no longer needed.[125]

Submissions and consultations

73.100 A number of stakeholders supported the proposal.[126] The Law Council of Australia strongly supported the inclusion of provisions which establish positive obligations of this kind. The Law Council also noted that Chapter 4 of the *Telecommunications (Interception and Access) Act* allows for the employees of telecommunications service providers to disclose voluntarily telecommunications data. The Law Council argued that, in these circumstances, it is important that there is a

---

123 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2)(a). See Ch 34.

124 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 21 May 2008.

125 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–2.

126 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; I Graham, *Submission PR 427,* 9 December 2007.

statutory obligation to review the information disclosed in a timely manner, to make an immediate assessment as to its relevance and to destroy it if it is not relevant.[127]

73.101 Some stakeholders did not think such an amendment was required.[128] For example, the AGD submitted that the destruction of irrelevant material already occurs in practice. The AGD also submitted that:

> It is worthwhile noting that investigations may span long periods of time and a law enforcement agency may not necessarily be able to determine whether the material is relevant until the investigation and any subsequent proceedings are completed.[129]

ALRC's view

73.102 Telecommunications data includes information about when, how and with whom individuals communicate and, in the case of mobile phones, location information. The voluntary disclosure of this information by employees of telecommunications service providers to ASIO and law enforcement agencies is a significant invasion of an individual's privacy. ASIO and law enforcement agencies, therefore, should be under a clear obligation to destroy telecommunications data when it is no longer needed for a permitted purpose.

73.103 While the retention of this information by law enforcement agencies may be regulated by the *Privacy Act*, in the interest of clarity and certainty, the *Telecommunications (Interception and Access) Act* should be amended to provide that ASIO and law enforcement agencies must destroy in a timely manner irrelevant material containing accessed telecommunications data which is no longer needed for a permitted purpose.

Recommendation 73–3 The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the Australian Security Intelligence Organisation and enforcement agencies must destroy in a timely manner irrelevant material containing accessed telecommunications data which is no longer needed for a permitted purpose.

Guidance

73.104 In DP 72, the ALRC proposed that, in the interests of transparency, the AGD should provide guidance on when the chief officer of an agency must cause information to be destroyed when it is no longer needed for a permitted purpose under ss 79 and 150 of the *Telecommunications (Interception and Access) Act*.[130]

---

127 Law Council of Australia, *Submission PR 527*, 21 December 2007.
128 Australian Federal Police, *Submission PR 545*, 24 December 2007.
129 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
130 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–2.

Submissions and consultations

73.105 A number of stakeholders supported the proposal.[131] The Law Council submitted that officers should be provided with guidance as to which purposes are 'permitted purposes' for their respective agency, and on how to determine the ongoing utility of any record obtained.[132] One stakeholder submitted that any guidance on destruction provided by the AGD would need to take into account the differences in the types of investigations undertaken by interception agencies.[133]

73.106 Other stakeholders provided qualified support for the proposal. One stakeholder supported the proposal, but noted that a legislative amendment is required as recommended by the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006.[134]

73.107 The AGD noted that it provides guidance to all agencies regarding the operation of the *Telecommunications (Interception and Access) Act* and that further guidance was provided to agencies through the inspection of the General Register relating to the warrant under which the record in question was created.[135]

ALRC's view

73.108 The ALRC accepts that there are currently no legislative timeframes within which agencies should review holdings of information and destroy information. There should be some broad guidance on timeframes, however, within which agencies should review and destroy information.

73.109 The ALRC accepts that the requirement to destroy information will vary according to the nature of the agency and the investigation. Guidance, rather than legislation, can accommodate these differences and provide flexibility about when information should be destroyed by an agency. This guidance should address the destruction of intercepted material, stored communications and telecommunications data.

73.110 The ALRC recommends below that the AGD should develop and, where appropriate, publish such guidance.[136]

Reporting requirements

73.111 Part 2–7 of the *Telecommunications (Interception and Access) Act* sets out various record-keeping and reporting requirements relating to intercepted telecommunications. For example, ss 80 and 81 of the Act require the chief officer of

---

131 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

132 Law Council of Australia, *Submission PR 527*, 21 December 2007.

133 Confidential, *Submission PR 488*, 19 December 2007.

134 I Graham, *Submission PR 427*, 9 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

135 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

136 Rec 73–5.

an agency to keep records of a number of matters, including particulars of each application for a warrant and details of each warrant issued to the agency.

73.112 Section 100 sets out a number of reporting requirements about agency warrants. Such requirements include: relevant statistics about applications for warrants that an agency made during the year; how many warrants included specified conditions or restrictions relating to the warrant; and the total number of telecommunication services intercepted under particular warrants.

73.113 Section 102 in Part 2–8 of the *Telecommunications (Interception and Access) Act* requires a report to set out information about the effectiveness of warrants, including the number of arrests and convictions recorded on the basis of lawfully intercepted information.

73.114 The reporting requirements relating to the use of stored communication warrants are contained in Part 3–5 of the *Telecommunications (Interception and Access) Act*. Section 151 requires an agency to keep records on various matters, including each stored communication warrant issued to the agency. Section 163 requires agencies to report on the effectiveness of stored communication warrants.[137]

73.115 In DP 72, the ALRC noted that the record-keeping and reporting requirements relating to access to stored communications are significantly less onerous than the requirements that apply to the interception of communications. For example, agencies are not required to provide as much information on the use and effectiveness of stored communication warrants as they are for interception warrants.[138] The ALRC asked whether the regime relating to access to stored communications under the *Telecommunications (Interception and Access) Act* should be amended to provide further reporting requirements relating to the use and effectiveness of stored communications warrants.[139]

Submissions and consultations

73.116 A number of stakeholders submitted that the reporting requirements relating to the use of stored communication warrants should be at least as rigorous as those relating to interception warrants.[140]

---

137 The reporting requirements relating to access to telecommunications data are contained in the *Telecommunications Act 1997* (Cth) pt 13 div 5. These requirements are discussed in Ch 71.

138 Compare *Telecommunications (Interception and Access) Act 1979* (Cth) ss 151 and 163 to Part 2–7 and s 102 of the Act. See discussion of the ASIO, agency and stored communication warrant regimes above.

139 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 64–4.

140 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Law Council of Australia, *Submission PR 527*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Confidential, *Submission PR 488*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

73.117 Other stakeholders did not support additional reporting requirements in relation to stored communication warrants.[141] For example, the AGD submitted that the annual reporting requirements for stored communications warrants and their effectiveness are similar to the requirements that apply to telecommunications interception warrants.[142]

ALRC's view

73.118 Sections 151 and 163 of the *Telecommunications (Interception and Access) Act* should be amended to provide for reporting requirements in relation to the use of stored communication warrants that are equivalent to the interception warrant reporting requirements under Part 2–7 and s 102 of the Act.[143] Reporting obligations are vital to providing adequate transparency and accountability of the interception and access regime set out under the *Telecommunications (Interception and Access) Act*. The ALRC can see no reason why stored communications warrants should be subject to less onerous reporting requirements than interception warrants, particularly given that more agencies can make applications for stored communications warrants than interception warrants.

Recommendation 73–4 Sections 151 and 163 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide for reporting requirements relating to the use of stored communication warrants that are equivalent to the interception warrant reporting requirements under Part 2–7 and s 102 of the Act.

Guidance

73.119 The *Telecommunications (Interception and Access) Act* provides for interception of, and access to, the content and substance of communications and other information about the communications. The content and substance of an individual's telephone conversations and other electronic communications, such as emails, are often private and sensitive. Further, information about when, how and with whom individuals communicate is also sensitive. Intelligence and law enforcement agencies, telecommunications service providers, regulators, oversight bodies, and the community should have a clear understanding about when communications may be intercepted and accessed, and how that information subsequently is to be handled.

---

141 Australian Federal Police, *Submission PR 545*, 24 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

142 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

143 The Senate Legal and Constitutional Affairs Committee Inquiry into provisions of the Telecommunications (Interception) Amendment Bill 2006 made a similar recommendation: Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [3.88], rec 11. Although the Telecommunications (Interception) Amendment Bill 2006 was amended to provide that reports on access to stored communications must contain information about the effectiveness of warrants, the record-keeping and reporting requirements for stored communications warrants are still less rigorous and detailed than those for other kinds of warrants.

73.120 There is currently very little published information on the interception and access of information under the *Telecommunications (Interception and Access) Act*. The AGD should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act*.

73.121 The guidance generally should address the interception and access of information under the *Telecommunications (Interception and Access) Act.* In this chapter, the ALRC has identified a number of issues, however, that should be addressed specifically in the guidance. These matters are:

- the definition of the term 'telecommunications data';
- when voluntary disclosure of telecommunications data to ASIO and enforcement agencies is permitted; and
- timeframes within which agencies should review holdings of information and destroy information.

Recommendation 73–5 The Australian Government Attorney-General's Department should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act 1979* (Cth), that addresses:

(a) the definition of the term 'telecommunications data';

(b) when voluntary disclosure of telecommunications data to the Australian Security Intelligence Organisation and other enforcement agencies is permitted; and

(c) timeframes within which agencies should review holdings of information and destroy information.

Oversight

73.122 A number of bodies have oversight of the interception and access of communications under the *Telecommunications (Interception and Access) Act*. As noted above, ASIO warrants are issued by the Attorney-General, and agency warrants are issued by a judge or a member of the AAT. The IGIS and the Commonwealth Ombudsman both have oversight roles in relation to interception and access of communications. Further, agencies that intercept and access communications under the Act also are subject to ministerial and parliamentary oversight.[144]

144 For further discussion of these accountability mechanisms see Chs 34 and 37.

Inspector-General of Intelligence and Security

73.123 The IGIS is an independent statutory officer who is responsible for ensuring that Australian intelligence agencies, such as ASIO, conduct their activities legally, behave with propriety, comply with any directions and guidelines from the responsible minister, and have regard for human rights, including privacy.[145] The IGIS, therefore, has oversight of ASIO in relation to the interception and access of communications under the *Telecommunications (Interception and Access) Act*.

73.124 The IGIS has stated that because B-Party interception warrants involve a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern, particular attention will be given to this type of warrant.[146]

73.125 The IGIS also has suggested that there may be a role for the IGIS in monitoring authorisations by ASIO officers to access prospective telecommunications data.[147] In DP 72, the ALRC noted that stakeholders had raised a range of issues relating to access to prospective telecommunications data, and asked whether the Telecommunications (Interception and Access) Amendment Bill 2007 (as it was then known) should be amended to provide that the IGIS monitor the use of powers by ASIO to obtain prospective telecommunications data.[148]

Submissions and consultations

73.126 A number of stakeholders supported such an amendment.[149] The AGD submitted that the IGIS already performs this function on an administrative basis in accordance with the terms of the *Inspector-General of Intelligence and Security Act 1986* (Cth). The AGD also noted that the *Telecommunications (Interception and Access) Act* does not contain specific provisions relating to the IGIS inspecting ASIO's telecommunications interception functions.[150]

ALRC's view

73.127 A legislative amendment to provide that the IGIS monitor the use of powers by ASIO to obtain prospective telecommunications data is unnecessary because the IGIS already has the power to perform this function under the *Inspector-General of Intelligence and Security Act.* The IGIS, however, should incorporate into his or her regular inspection program oversight of the use of powers to obtain prospective telecommunications data by ASIO. The power to obtain access to prospective

---

145 For a detailed discussion of the Inspector General of Intelligence and Security see Ch 34.

146 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [4.17].

147 Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), [3.66].

148 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 63–2(d).

149 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Law Council of Australia, *Submission PR 527*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

150 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

telecommunications has significant privacy implications and should be subject to stringent control and oversight.[151]

Commonwealth Ombudsman

73.128 The Commonwealth Ombudsman is an independent statutory office established by the *Ombudsman Act 1976* (Cth). The Act provides that the Ombudsman is to investigate the administrative actions of Australian Government departments and prescribed authorities in response to complaints, or on the Ombudsman's own motion.

73.129 The Commonwealth Ombudsman has oversight of law enforcement bodies, such as the Australian Federal Police, that access and intercept communications under the *Telecommunications (Interception and Access) Act*.[152] Further, the Commonwealth Ombudsman has specific powers under the *Telecommunications (Interception and Access) Act* to enter premises occupied by agencies, obtain relevant material, inspect records and prepare reports in relation to the interception of, or access to, communications.[153]

Submissions and consultations

73.130 The Law Council of Australia submitted that no equivalent to s 87 of the *Telecommunications (Interception and Access) Act* exists in relation to stored communication warrants. Section 87 provides, among other things, that the Ombudsman may require an officer of an agency to give information to the Ombudsman and to attend a specified place in order to answer questions relevant to the inspection of interception records; and where the Ombudsman does not know the officer's identity, require the chief officer of an agency, or a person nominated by the chief officer, to answer questions relevant to the inspection.

ALRC's view

73.131 The Ombudsman should have the same powers to inspect records and to compel the presence of officers to answer questions relevant to the inspection of records, regardless of whether the records relate to intercepted or stored communications. It is arguable that the Ombudsman would have the power to obtain this information under the general provisions of the *Ombudsman Act 1976* (Cth). In the interest of clarity, however, the ALRC recommends that the same power under s 87 of the *Telecommunications (Interception and Access) Act* should apply in relation to stored communication warrants.

---

151 The Senate Legal and Constitutional Affairs Committee inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 made a similar recommendation: Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), rec 3.

152 See, eg, *Ombudsman Act 1976* (Cth) ss 5–7.

153 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.7, pt 3.5 div 2.

Recommendation 73–6 The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide expressly that where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection of the agency's records relating to access to a stored communication, the Ombudsman may:

(a) require the officer to give the information to the Ombudsman and to attend a specified place in order to answer questions relevant to the inspection; and

(b) where the Ombudsman does not know the officer's identity, require the chief officer, or a person nominated by the chief officer, to answer questions relevant to the inspection.

Public Interest Monitor

73.132 One issue for consideration is whether the interception of, and access to, communications under the *Telecommunications (Interception and Access) Act* requires additional oversight. One option, suggested by the OVPC,[154] was the establishment of a public interest monitor (PIM).

73.133 A PIM was established in Queensland under the *Crime and Misconduct Act 2001* (Qld), and the *Police Powers and Responsibilities Act 2000* (Qld). Under the *Crime and Misconduct Act*, the PIM monitors applications for, and the use of, surveillance warrants and covert search warrants.[155] Under the *Police Powers and Responsibilities Act*, the PIM monitors applications for, and the use of, surveillance device warrants, retrieval warrants and covert search warrants.[156]

73.134 The PIM's primary role is to represent the public interest where law enforcement agencies seek approval to use search powers and surveillance devices that have the capacity to infringe the rights and civil liberties of citizens. The role is based on the public interest in ensuring that law enforcement agencies meet all legislative requirements, and that their proposed actions do not extend beyond the parameters laid down by the Queensland Parliament.

73.135 PIMs perform a variety of functions. For example, under the *Crime and Misconduct Act*, the PIM's functions include: appearing at any hearing of an application to a Supreme Court judge or magistrate for a surveillance warrant or covert search warrant to test the appropriateness and validity of the application; monitoring the Queensland Crime and Misconduct Commission's compliance with matters concerning applications for surveillance warrants and covert search warrants; gathering

---

154 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007 referring to Office of the Victorian Privacy Commissioner, *Submission to the Australian Government Attorney-General's Department's Review of the Regulation of Access to Communications*, May 2005.

155 *Crime and Misconduct Act 2001* (Qld) s 324(1).

156 *Police Powers and Responsibility Act 2000* (Qld) s 740(1).

statistical information about the use and effectiveness of surveillance warrants and covert search warrants; and issuing an annual report.[157]

73.136 In DP 72, the ALRC expressed the preliminary view that there is adequate oversight of the interception and access of communications under the *Telecommunications (Interception and Access) Act*, but noted that it was interested in stakeholder views on the need for a PIM. The ALRC asked whether the *Telecommunications (Interception and Access) Act*) should be amended to provide for the role of a public interest monitor, and if so, whether its role should include:

- appearing at any application made by an agency for interception and access warrants under the Act;
- testing the validity of warrant applications;
- gathering statistical information about the use and effectiveness of warrants;
- monitoring the retention or destruction of information obtained under a warrant;
- providing to the IGIS, or other authority as appropriate, a report on non-compliance with the Act; or
- reporting to the Australian Parliament on the use of interception and access warrants.[158]

Submissions and consultations

73.137 A number of stakeholders supported an amendment of the *Telecommunications (Interception and Access) Act* to provide for the role of a PIM.[159] The Law Council of Australia submitted that the current oversight mechanisms are directed at reviewing interception and access powers after they have been exercised. The Law Council argued that a PIM may bring a greater degree of scrutiny to bear on the grounds advanced for seeking a warrant and for claiming that it is a necessary and justified intrusion into the privacy of individuals.[160] One stakeholder submitted that if the *Telecommunications (Interception and Access) Act* is not amended to establish a PIM, it should be amended to require notification to individuals within 90 days of the cessation of the interception.[161]

---

157 *Crime and Misconduct Act 2001* (Qld) ss 11, 122(1)(b), 149(b), 326–328. See also *Police Powers and Responsibility Act 2000* (Qld) ss 212, 220, 335, 357, 740–745.

158 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 64–5.

159 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007.

160 Law Council of Australia, *Submission PR 527*, 21 December 2007. The Law Council emphasised that if a PIM were to be involved in the application process, this would not relieve the judicial officer or AAT member from having to satisfy himself or herself personally, based on the evidence presented, of each of the matters set out in the legislation.

161 I Graham, *Submission PR 427*, 9 December 2007.

73.138 Other stakeholders did not support the establishment of a PIM.[162] The Australian Federal Police submitted that a PIM is not required because the existing oversight requirements in the Act are adequate.[163] The AGD submitted that the introduction of a PIM at the application stage could raise questions about the integrity and independence of the warrant issuing authority, which could affect proceedings instituted at a later time. The AGD also noted that there is no prohibition on a PIM being involved in agencies' investigations before an application for a warrant is made. This would need to be done on an agency-by-agency basis and before an application is put before an issuing authority.

> Processes similar to this are used by a number of law enforcement agencies. For example, a member of a police force may consult the relevant Director of Public Prosecutions before making an application to an issuing authority. This consultation could include whether an application for a warrant is merited.[164]

73.139 The AGD submitted that it is responsible for obtaining and collating statistical information from the agencies that are able to apply for warrants under the Act; and that the relevant oversight body in each state and territory, and the Commonwealth Ombudsman, are responsible for monitoring and reporting on the compliance by agencies with the record keeping, reporting and destruction of information requirements of the Act.[165]

ALRC's view

73.140 Many of the functions outlined in the question asked in DP 72 are currently exercised by existing bodies. The ALRC acknowledges, however, that these bodies review interception or access after it has taken place. The ALRC sees merit in having the public interest represented before the warrant is issued.

73.141 A PIM would ensure a greater degree of accountability, and would enhance the integrity and independence of the warrant-issuing process. This issue, however, should be the subject of further consultation. In Chapter 71, the ALRC recommends that the Australian Government initiate a review of telecommunications legislation, and that the review should consider whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a PIM.[166]

Office of the Privacy Commissioner

73.142 Stakeholders have submitted that the OPC should have a more visible and formally recognised role in the formation of policies affecting telecommunications and law enforcement.[167] The Australian Privacy Foundation has noted that the Privacy

---

162 Confidential, *Submission PR 488*, 19 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.
163 Australian Federal Police, *Submission PR 545*, 24 December 2007.
164 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
165 Ibid.
166 See Rec 71–2.
167 Australian Mobile Telecommunications Association, *Submission PR 154*, 30 January 2007.

Commissioner has been excluded from the deliberations of the ACMA Law Enforcement Advisory Committee.[168]

73.143 The Law Enforcement Advisory Committee assists ACMA in performing its telecommunications functions as set out in s 8 of the *Australian Communications and Media Authority Act 2005* (Cth), by providing advice and recommendations to ACMA on law enforcement and national security issues relating to telecommunications. The Committee meets on a quarterly basis and is made up of representatives from law enforcement and national security agencies, carriers and carriage service providers, the Department of Broadband, Communications and the Digital Economy (DBCDE), and the AGD. In DP 72, the ALRC proposed that the OPC should be a member of the ACMA Law Enforcement Advisory Committee.[169]

Submissions and consultations

73.144 A number of stakeholders supported the proposal.[170] For example, the OPC submitted that providing a formal role for the OPC on the ACMA Law Enforcement Advisory Committee would help to ensure that the privacy impact of policy proposals were given appropriate weight.[171]

73.145 ACMA submitted that it is currently reviewing the ongoing operation and membership of the Law Enforcement Advisory Committee, and is considering comments received on this issue.[172] The AGD submitted that membership of the Law Enforcement Advisory Committee is a matter for ACMA.[173] One stakeholder opposed the proposal.[174]

ALRC's view

73.146 The OPC currently has the capacity to be involved in reviews of the *Telecommunications (Interception and Access) Act.* In the ALRC's view, however, the OPC should have a more formal role in relation to law enforcement issues relating to telecommunications.

---

168 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

169 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–4.

170 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Federal Police, *Submission PR 545*, 24 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

171 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

172 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007. See also Optus, *Submission PR 532*, 21 December 2007.

173 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

174 AAPT Ltd, *Submission PR 338*, 7 November 2007.

73.147 The OPC should be a member of the ACMA Law Enforcement Advisory Committee. Membership on this Committee would complement the OPC's legislative scrutiny function.[175] It also would complement the power recommended in Chapter 47 to allow the Privacy Commissioner to direct an agency to carry out a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[176]

Recommendation 73–7 The Australian Communications and Media Authority should add the Office of the Privacy Commissioner as a member of the Law Enforcement Advisory Committee.

State and territory oversight

73.148 One stakeholder submitted that the ALRC should consider the oversight of access to stored communications by state and territory agencies. She noted that stored communication warrants can be issued by state or territory magistrates, and that the provisions concerning disclosure, use and reporting do not appear to be enforceable by the Commonwealth, or subject to any oversight by state or territory ministers or parliaments. She noted that this issue does not arise in relation to intercepted information because there is a requirement that the states and territories enact complementary interception legislation.[177]

73.149 This issue was considered by the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006. The Committee recommended that, consistent with the existing arrangements for telecommunications interception, immediate action should be taken to ensure the enforceability of the stored communications provisions on state and territory agencies by requiring complementary legislation to be enacted as a precondition to being granted the powers of an enforcement agency under the stored communications regime.[178]

73.150 In its response to the recommendation, the Australian Government stated that the oversight mechanisms in the Act are adequate for the proper operation of the Act, and it did not accept that complementary state or territory legislation should be a pre-condition for access to stored communications. The Government accepted that there should be further consideration of this recommendation following a reasonable operational timeframe of the stored communications regime.[179]

---

175 *Privacy Act 1988* (Cth) s 27.

176 Rec 47–4.

177 I Graham, *Submission PR 427*, 9 December 2007.

178 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [3.67], rec 6.

179 *Australian Government Response to Australia—Senate Legal and Constitutional Legislation Committee Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), 4.

73.151 It is essential that the Australian Government has the ability to enforce the obligations on state and territory agencies prescribed in the *Telecommunications (Interception and Access) Act* relating to accessing stored communications. In the ALRC's view, complementary state or territory legislation relating to access to stored communications should be considered as part of the review of telecommunications legislation recommended in Chapter 71.

Spam and telemarketing

73.152 'Spam' refers to the use of electronic messaging systems to send unsolicited commercial messages. While the most widely recognised form of spam is email spam, the term also is applied to similar activities in other electronic media, including instant messaging, mobile phone messaging and short message service (SMS) messaging.

73.153 Spam has the potential to threaten the viability and efficiency of electronic messaging by damaging consumer confidence, obstructing legitimate business activity and imposing costs on users.[180] It was recently noted that:

> Spam's growth has been metastatic, both in raw numbers and as a percentage of all mail. In 2001, spam accounted for about five per cent of the traffic on the Internet; by 2004, that figure had risen to more than seventy per cent. This year [2007], in some regions, it has edged above ninety per cent—more than a hundred billion unsolicited messages clogging the arterial passages of the world's computer networks every day.[181]

73.154 'Telemarketing' is the marketing of goods and services to the consumer by telephone. Many Australians consider spam and telemarketing to be an invasion of their privacy. In 2006–07, the Telecommunications Industry Ombudsman (TIO) reported that it had received 680 complaints about telemarketing.[182] In that same year, ACMA received 1,831 written complaints related to spam.[183]

73.155 A large number of submissions to the current Inquiry raised concerns about spam and telemarketing.[184] On 1–2 June 2006, the ALRC invited members of the public to contact the ALRC to provide their views and experiences of privacy protection in Australia. This initiative—the National Privacy Phone-In—attracted widespread media coverage, which prompted a large community response. In total, the

---

180 National Office for the Information Economy, *Spam Act 2003: A Practical Guide for Business* (2004), 2.

181 M Specter, 'Damn Spam', *The New Yorker* (online), 6 August 2007, <www.newyorker.com>.

182 Telecommunications Industry Ombudsman, *Annual Report 2006–07* (2007), 54. This is a 60% drop in the number of complaints from the previous year. The TIO attributes this to the introduction of the Do Not Call Register. The Do Not Call Register is discussed below.

183 Australian Communications and Media Authority, *Annual Report 2006–07* (2007), 52.

184 See, eg, A Jackson, *Submission PR 142*, 24 January 2007; L Thomas, *Submission PR 65*, 9 December 2006; G Campbell, *Submission PR 54*, 9 October 2006; N Keele, *Submission PR 53*, 9 October 2006; L Mitchell, *Submission PR 46*, 2 June 2006; P Wikramanayake, *Submission PR 45*, 1 June 2006; J Dowse, *Submission PR 44*, 2 June 2006; L O'Connor, *Submission PR 35*, 2 June 2006; Confidential, *Submission PR 31*, 3 June 2006; M Rickard, *Submission PR 19*, 1 June 2006; Confidential, *Submission PR 13*, 26 May 2006.

ALRC received 1,343 responses. The great majority of respondents (73%) nominated telemarketing as their main concern.[185] A large number of respondents to the National Privacy Phone-In also considered spam to be an interference with their privacy.[186]

Should the *Privacy Act* regulate spam and telemarketing?

73.156 Many small businesses that use spam or engage in telemarketing are exempt from compliance with the *Privacy Act*.[187] Further, the definition of 'personal information' in the *Privacy Act* may not cover information that enables individuals to be contacted, such as email addresses that do not contain a person's name.[188]

73.157 In addition, NPP 2 does not apply to, or restrict, the use of personal information for the primary purpose for which it was collected, which could be to engage in telemarketing. NPP 2.1 also expressly authorises organisations to use personal information for the secondary purpose of direct marketing (which includes telemarketing) in certain circumstances—although an organisation that uses information in this way must offer the individual an option to refuse any further direct marketing communications.

73.158 For these reasons, the *Privacy Act* has left unregulated some practices in the telecommunications context that interfere with privacy. Accordingly, two pieces of federal legislation were introduced to regulate specific activities that impact on privacy in the telecommunications context—the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).

73.159 The ALRC considers that the *Spam Act* and the *Do Not Call Register Act* should continue to regulate spam and telemarketing. There is a strong view in the community that some forms of direct marketing are more intrusive than others and should be subject to stronger regulation than applies to less intrusive forms of direct marketing.

73.160 In light of the recent review of the *Spam Act* by the then Department of Communications, Information Technology and the Arts (DCITA),[189] the introduction of the *Do Not Call Register Act* and the Senate Environment, Communications, Information Technology and the Arts Committee inquiry into that Act,[190] the ALRC does not propose to conduct another detailed study of the *Spam Act* and the *Do Not Call Register Act*. The following section does consider, however, how they interact with the *Privacy Act*.

---

185 This possibly was influenced by the fact that a number of media stories about the National Privacy Phone-In focused on telemarketing as a possible concern.

186 See, eg, *ALRC National Privacy Phone-in*, June 2006, Comment #9.

187 *Privacy Act 1988* (Cth) ss 6C, 6D. The small business exemption is discussed in Ch 39.

188 The definition of 'personal information' is discussed in Ch 6.

189 Australian Government Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006). Now the Australian Government Department of Broadband, Communications and the Digital Economy.

190 Australian Parliament—Senate Environment, Communications, Information Technology and the Arts Committee, *Inquiry into the provisions of the Do Not Call Register Bill 2006 and the Do Not Call Register (Consequential Amendments) Bill 2006* (2006).

Spam Act

73.161 The *Spam Act* prohibits the sending of commercial electronic messages via email, SMS, multimedia message service or instant messaging without the consent of the receiver. Accordingly, it establishes an opt-in regime that is different from the provisions governing the use of information for direct marketing in the *Privacy Act*.[191]

73.162 The definitions of 'consent' in the *Privacy Act* and the *Spam Act* are broadly consistent. The *Privacy Act* provides that 'consent' means 'express consent or implied consent'.[192] Under the *Spam Act*, however, consent can be express and inferred, although it may not be inferred from the mere publication of an electronic address.[193] Consent can be inferred from 'conspicuous publication' of certain electronic addresses, such as the electronic addresses of employees, directors or officers of organisations, so long as the publication is not accompanied by a statement to the effect that the account holder does not wish to receive unsolicited commercial electronic messages.[194] Regulations may specify in more detail the circumstances in which consent may or may not be inferred.[195] Consent can be withdrawn if the account holder or a user of the account indicates that he or she does not wish to receive any further commercial electronic messages.[196]

73.163 The *Spam Act* does not prohibit sending 'designated commercial electronic messages'. A commercial electronic message is a 'designated commercial electronic message' if it consists of no more than factual information,[197] or the message is authorised by:

- a government body, registered political party, religious organisation, a charity or charitable institution, and the message relates to goods or services, and the body is the supplier, or prospective supplier, of the goods or services concerned;[198] or
- an educational institution, and the account holder is, or has been, enrolled as a student in that institution or is a member or former member of the household of the relevant electronic account holder and is, or has been, enrolled as a student in that institution, and the message relates to the supply of goods or services, and the educational institution is the supplier, or prospective supplier, of the goods or services concerned.[199]

---

191 *Spam Act 2003* (Cth) s 16. Direct marketing is discussed further in Ch 26.
192 *Privacy Act 1988* (Cth) s 6.
193 *Spam Act 2003* (Cth) sch 2 cl 4. Consent is discussed further in Ch 19.
194 Ibid sch 2 cl 4.
195 Ibid sch 2 cl 5.
196 Ibid sch 2 cl 6.
197 Ibid sch 1 cl 2.
198 Ibid sch 1 cl 3.
199 Ibid sch 1 cl 4.

73.164 The *Spam Act* requires lawful commercial electronic messages to contain certain information, such as information about the identity and contact details of the sender.[200] It also provides that a person must not send a commercial electronic message unless the message includes a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the message, or a statement to a similar effect.[201] The requirement to include an unsubscribe message does not apply to designated commercial electronic messages.[202]

73.165 The *Spam Act* also contains rules prohibiting the supply and use of 'address-harvesting software'[203]—that is, software that is used to search the internet for electronic addresses to compile or 'harvest'.[204] Ordinary telephone calls and facsimile communications are not covered by the Act.[205] ACMA has a range of powers to enable it to enforce the provisions of the *Spam Act*.[206]

73.166 Two industry codes dealing with spam have been developed under the *Telecommunications Act* since the introduction of the *Spam Act*. These are the *Australian eMarketing Code of Practice*[207] and the *Internet Industry Code of Practice*.[208] These codes are intended to complement the operation of the *Spam Act* by outlining action to be taken by industry members to help to counter spam.

73.167 In 2006, the Federal Court of Australia delivered the first significant decision dealing with the *Spam Act*. In *Australian Communications and Media Authority v Clarity1 Pty Ltd*, the Court found that the respondents (Clarity1 and the company's director, Wayne Mansfield) had sent tens of millions of messages to recipients whose email addresses had been obtained by the use of harvested address lists.[209] The respondent raised a number of defences which were unsuccessful, including that the recipients of the messages had consented to the sending of the messages because they failed to use the 'unsubscribe facility' in the messages.

73.168 The respondents sought to rely on the OPC's *Guidelines to the National Privacy Principles*, which provide in relation to NPP 2 that 'it may be possible to infer consent from the individual's failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up'.[210] Nicholson J did not accept this argument, finding that non-legislative guidelines do not assist in the interpretation of legislation. Nicholson J also held that the inclusion of an unsubscribe facility in a

---

200 Ibid s 17.
201 Ibid s 18.
202 Ibid s 18(1)(b).
203 Ibid pt 3.
204 Ibid s 4.
205 Ibid s 5(5); *Spam Regulations 2004* (Cth) cl 2.1.
206 *Spam Act 2003* (Cth) pt 4; *Telecommunications Act 1997* (Cth) pt 28. See also Australian Government Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006), ch 11.
207 Australian eMarketing Code Development Committee, *Australian eMarketing Code of Practice* (2005).
208 Internet Industry Association, *Internet Industry Spam Code of Practice* (2006).
209 *Australian Communications and Media Authority v Clarity1 Pty Ltd* (2006) 150 FCR 494.
210 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 37.

commercial electronic message does not support an inference that a recipient consented to receiving a message by failing to use the facility.[211]

73.169 In its review of the private sector provisions of the *Privacy Act* (OPC Review), the OPC indicated it would discuss with the Australian Communications Authority (ACA) (now ACMA) the development of guidance to clarify the relationship between the *Privacy Act* and the *Spam Act*.[212]

73.170 In 2006, DCITA concluded a review of the operation of the *Spam Act*.[213] DCITA found that the Act was operating successfully and should not be amended. It recommended, however, that additional advice be developed on the operation of certain aspects of the Act. It also recommended that steps be taken to educate the public about the operation of the Act. To this end, it recommended that the OPC and ACMA develop 'joint awareness materials to clarify the relationship between the *Spam Act* and the *Privacy Act*'.[214] DCITA also recommended that the Australian Government undertake further consultation to determine whether facsimile communications should be regulated by the *Spam Act*.

73.171 In DP 72, the ALRC noted that a number of stakeholders had raised issues relating to the *Spam Act*. Stakeholders submitted that the *Spam Act* and the *Privacy Act* were inconsistent because the *Spam Act* adopts an opt-in model, while the *Privacy Act* provides an opt-out model for direct marketing. Stakeholders also submitted that the *Spam Act* and the *Privacy Act* take different approaches to consent, and that consideration should be given to whether the *Spam Act* should regulate Bluetooth messages.[215]

73.172 The ALRC expressed the preliminary view that the *Spam Act* is an appropriate response to public concern about unsolicited commercial electronic messages. The ALRC noted, however, that it was interested in views on whether the *Spam Act* should be amended to:

- provide that the definition of 'electronic message' under s 5 includes Bluetooth messages;
- provide that facsimile messages are regulated under the Act;
- provide that an electronic message is required to include an unsubscribe message if the electronic message: consists of no more than factual information; has been authorised by a government body, a registered political party, a

---

211 *Australian Communications and Media Authority v Clarity1 Pty Ltd* (2006) 150 FCR 494, [80].

212 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 11.

213 Australian Government Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006).

214 Ibid, rec 22.

215 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [64.79]–[64.85].

religious organisation, a charity or charitable institution, or an educational institution, and relates to goods or services; or

- remove the exception for registered political parties.[216]

Submissions and consultations

73.173 The DBCDE submitted that the ALRC's question appears to go beyond the scope of the ALRC's Terms of Reference, and suggested that the ALRC may wish to refrain from further examination of the *Spam Act*. The Department noted that the prohibition in the *Spam Act* on unsolicited commercial electronic messages applies to messages sent to private individuals, organisations, government agencies and businesses.

> The possible amendments in relation to which the ALRC is seeking comment would therefore have a much broader impact than just affecting privacy law. In particular, the amendments would impact on business to business dealings and business to Government dealings.[217]

73.174 The DBCDE also noted that the review of the *Spam Act* included consideration of the issues raised by the ALRC,[218] and that it is reviewing whether the scope of the *Spam Act* should be extended to cover facsimile messages.[219]

73.175 A number of stakeholders supported Bluetooth messages being regulated under the *Spam Act*.[220] Others stakeholders did not support this reform.[221] For example, ACMA highlighted that consumers can control the receipt of Bluetooth messages to a greater extent than SMS or email, without losing functionality.[222] The DBCDE submitted that a commercial electronic message needs to be sent to an address connected with an account to be regulated under the *Spam Act*. With Bluetooth technology, however, the device itself and not an account is used to receive the message. The Department also noted that it is not aware of widespread public concern in relation to the volume or impact of commercial electronic messages sent to Bluetooth devices.[223]

---

216 Ibid, Question 64–6.

217 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

218 Australian Government Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006).

219 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

220 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

221 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

222 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

223 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

73.176 Some stakeholders supported facsimile messages being regulated under the *Spam Act*.[224] Other stakeholders stated that they were unaware of any significant issues with the use of facsimile messages for marketing purposes to warrant any legislative or regulatory action.[225] The DBCDE noted that it is considering this issue.[226]

73.177 A number of stakeholders supported the notion that a wider range of messages—including messages that consist of no more than factual information, or that have been authorised by a government body, a registered political party, a religious organisation, a charity or educational institution—should include an unsubscribe facility.[227] Other stakeholders submitted that amending the *Spam Act* so that purely factual messages must include an unsubscribe facility would have a detrimental impact on customer service.[228] The DBCDE noted that submissions to the review of the *Spam Act* indicated that there is little community concern about these kinds of messages.[229]

73.178 Some stakeholders supported the removal of the registered political party exemption from the *Spam Act*.[230] The DBCDE submitted, however, that the exemption is consistent with other exemptions in the legislation which seek to balance the ability of organisations that undertake socially important work in the 'public interest' and the rights of individuals to privacy. The DBCDE submitted that messages from political parties typically take place during a limited period, such as during an election campaign. The Department also noted that the removal of the exemption was examined by the *Spam Act* review, which found that the exemption has caused few difficulties in practice and recommended that it should be retained.[231]

---

224 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007.

225 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

226 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

227 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

228 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See also Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

229 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

230 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

231 Australian Government Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006); Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

ALRC's view

73.179 The ALRC does not make any recommendations to amend the *Spam Act*, as these issues were recently considered in the review of the Act. Further, the DBCDE is considering whether the scope of the Act should be extended to cover facsimile messages.

73.180 The *Spam Act* is an appropriate response to public concern about unsolicited commercial electronic messages. There is some confusion, however, about the interaction between the *Privacy Act* and the *Spam Act*. The ALRC recommends below that ACMA, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry, including guidance on the interaction between the *Privacy Act* and the *Spam Act*.

73.181 The ALRC notes stakeholder concerns about the different approaches to consent under the *Privacy Act* and the *Spam Act*. The guidance should address the requirements to obtain an individual's consent for the purposes of the *Privacy Act* and the *Spam Act*—including how it applies in various contexts and when it is appropriate to use the mechanism of 'bundled consent'.[232]

Do Not Call Register Act

73.182 On 3 May 2007, the then Minister for Communications launched the national Do Not Call Register.[233] The scheme was established under the *Do Not Call Register Act*, which enables the holder of an account for an Australian telephone number to elect not to receive unsolicited telemarketing calls. The Act was introduced in response to 'rising community concerns about the inconvenience and intrusiveness of telemarketing, as well as concerns about the impact of telemarketing on an individual's privacy'.[234]

73.183 The *Do Not Call Register Act* enables account holders, and nominees of account holders, to apply to have their telephone numbers included on a Do Not Call Register held by ACMA. This establishes an opt-out regime that is different from the provisions governing the use of information for direct marketing in the *Privacy Act*.[235] The *Privacy Act* prohibits the use of personal information for the secondary purpose of direct marketing unless an organisation draws an individual's attention to the fact that he or she may opt out of any further direct marketing. The Act also prohibits direct marketing to an individual who has made a request not to receive direct marketing communications. The *Do Not Call Register Act*, however, prohibits the making of

---

232 See discussion of bundled consent in Ch 19.

233 Australian Communications and Media Authority, 'Do Not Call Register Launched' (Press Release, 3 May 2007).

234 Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth). The OPC Review recommended that the Australian Government consider amending the *Privacy Act* to provide consumers with a right to opt out of receiving all forms of direct marketing at any time, and establishing a 'Do Not Contact' register: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 23, 25.

235 *Do Not Call Register Act 2006* (Cth) ss 13–15. Direct marketing is discussed further in Ch 26.

unsolicited telemarketing calls without consent to a telephone number on the Do Not Call Register.[236]

73.184 The definitions of 'consent' under the *Privacy Act* and the *Do Not Call Register Act* are broadly consistent. As noted above, under the *Privacy Act* consent may be express or implied. Under the *Do Not Call Register Act*, consent can be express or inferred, although it cannot be inferred simply from the publication of the telephone number.[237] Regulations may specify in more detail circumstances in which consent may or may not be inferred.[238] If express consent is given, and it is not given for a specified period or for an indefinite period, it is taken to have been withdrawn after three months.[239]

73.185 'Designated telemarketing calls' are exempt from the prohibition on making unsolicited telemarketing calls to a number registered on the Do Not Call Register. 'Designated telemarketing calls' include certain calls authorised by: government bodies; religious organisations; charities or charitable institutions; registered political parties; independent members of the Commonwealth Parliament, a state parliament, or the legislative assembly for an Australian territory, or a local governing body, or a candidate in an election; or educational institutions.[240] In addition, certain telephone numbers—such as numbers used exclusively for the sending or receiving of facsimile communications—cannot be included on the register.[241]

73.186 Telemarketers can request information from ACMA about whether a particular telephone number is on the register.[242] Numbers are registered for a period of three years, after which they are removed from the register unless another valid application for registration of the number is made.[243]

73.187 ACMA has a range of powers to enable it to enforce the provisions of the *Do Not Call Register Act*.[244] In addition, ACMA is required to establish a national industry standard to regulate the conduct of telemarketers, including those exempt from the operation of the Act.[245] On 22 March 2007, ACMA made the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Standard 2007*.[246] The Standard establishes minimum standards in four main areas:

---

236 Ibid s 11. Consent is discussed further in Ch 19.
237 Ibid sch 2 cl 4.
238 Ibid sch 2 cl 5.
239 Ibid sch 2 cl 3.
240 Ibid sch 2–5.
241 Ibid s 14.
242 Ibid s 20.
243 Ibid s 17.
244 *Do Not Call Register (Consequential Amendments) Act 2006* (Cth) sch 1 pt 2.
245 *Telecommunications Act 1997* (Cth) s 125A.
246 *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Standard 2007*. The standard commenced on 31 May 2007.

- restricting the calling hours and days for making telemarketing and research calls;
- requiring provision of specific information by the caller;
- providing for the termination of calls; and
- requiring callers to enable calling line identification.[247]

73.188 There is an exception to the rules where consent has been given in advance by the call recipient to receive the call during the prohibited calling hours.[248]

73.189 In DP 72, the ALRC noted that a number of stakeholders had raised issues relating to the *Do Not Call Register Act*. These issues primarily concerned the different requirements for consent under the two Acts and the authorised exceptions for designated telemarketing calls for politicians and electoral candidates.[249] The ALRC expressed the view that the definitions of 'consent' under the *Privacy Act* and the *Do Not Call Register Act* are broadly consistent. The ALRC asked whether the *Do Not Call Register Act* should be amended to remove the exception for registered political parties, independent members of parliament and candidates in an election.[250]

Submissions and consultations

73.190 Two stakeholders supported the removal of the exemption relating to politicians and electoral candidates.[251] The DBCDE submitted that the removal of the exemption from the Act would be premature.

73.191 The Department also noted that it is closely monitoring the impact of the exemption on individuals who have placed their numbers on the Do Not Call Register. The DBCDE submitted that it has received a small number of complaints about the impact of the exemption. It noted that the exemption will be considered as part of the legislative review scheduled to commence in 2010.[252]

ALRC's views

73.192 The *Do Not Call Register Act* is an appropriate response to public concern about telemarketing. This is confirmed by the latest complaint statistics released by the TIO. In 2006–07, the TIO reported a 60% decrease in the number of complaints relating to telemarketing which it attributes to the introduction of the Do Not Call Register.[253]

---

247 Ibid ss 5–8.
248 Ibid s 5(5).
249 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [64.102]–[64.107].
250 Ibid, Question 64–7.
251 I Graham, *Submission PR 427*, 9 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.
252 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.
253 Telecommunications Industry Ombudsman, *Annual Report 2006–07* (2007), 54–55.

73.193 In Chapter 41, the ALRC recommends the removal of the political exemption from the *Privacy Act*. The ALRC accepts, however, that it may be too early to recommend the removal of the exemption relating to politicians and electoral candidates from the *Do Not Call Register Act*. The ALRC notes that the DBCDE is monitoring the impact of the exemption on individuals who have placed their numbers on the Do Not Call Register. The ALRC agrees that this issue should be considered as part of the legislative review scheduled to commence in 2010.

73.194 Concerns were expressed in submissions about the different approaches to consent under the *Privacy Act* and the *Do Not Call Register Act*. The definitions of consent under both Acts are broadly consistent. The *Do Not Call Register Act* contains additional requirements in relation to consent, including that consent is taken to have been withdrawn at the end of three months. This requirement ensures that telemarketers cannot continue to contact account holders after the time period has elapsed.

73.195 Submissions indicate, however, that more guidance is required. The ALRC has recommended that the guidance on privacy in the telecommunications industry should address the interaction between the *Privacy Act* and the *Do Not Call Register Act*.[254] The guidance should address the requirements to obtain an individual's consent for the purposes of the *Privacy Act* and the *Do Not Call Register Act*.

Telecommunications regulators

73.196 Several bodies are involved in the regulation of the telecommunications industry. ACMA is a statutory authority[255] with specific regulatory powers conferred on it by a number of Acts, including the *Telecommunications Act*, *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth), *Spam Act* and the *Do Not Call Register Act*.

73.197 The TIO is an external dispute resolution scheme that investigates and determines complaints by users of carriage services,[256] including complaints about breaches of the NPPs.[257] The OPC also deals with complaints of interference with privacy in the telecommunications industry.

73.198 The Commonwealth Ombudsman inspects, and reports on, actions taken under the *Telecommunications (Interception and Access) Act* by Commonwealth law enforcement agencies.[258] The IGIS also has various oversight powers under the *Telecommunications (Interception and Access) Act*.[259]

---

254 Rec 73–10.
255 *Australian Communications and Media Authority Act 2005* (Cth) s 8(1).
256 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 128(4).
257 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, cl 4.1.
258 Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007.
259 See discussion of the IGIS above.

73.199 Each of these regulatory bodies receives privacy-related complaints from consumers. ACMA noted that concern about privacy was a theme in a number of the complaints it received in 2006–07.[260] In this same period, the TIO received 2,343 complaints relating to privacy of consumers with a landline, mobile telephone or internet connection. Many of these complaints related to telemarketing.[261] In 2006–07, the OPC received 81 complaints about privacy in the telecommunications sector (approximately 10% of all complaints) and 756 telephone enquires about privacy in the telecommunications sector (approximately 10% of all NPP telephone enquiries).[262]

73.200 These regulatory bodies have different powers to resolve complaints. For example, the TIO has the power to order service providers to provide complainants with compensation of up to $10,000.[263] There is no statutory limit on the amount of compensation that the Privacy Commissioner can award to a complainant.[264]

73.201 Stakeholders making submissions to the OPC Review noted that the existence of multiple regulators in the telecommunications industry had the potential to: confuse consumers wishing to complain about telecommunications privacy issues; delay or complicate the resolution of complaints;[265] and waste agency resources.[266] Telstra suggested that industry complaint-handling bodies be given responsibility for considering privacy-related complaints at first instance. It submitted that this would ensure the efficient and timely investigation of complaints and enable the OPC to focus on broader privacy issues.[267] The OPC noted that it could work closely with other

---

260 Australian Communications and Media Authority, *Annual Report 2006–07* (2007), 60.

261 Telecommunications Industry Ombudsman, *Annual Report 2006–07* (2007), 54–55. Communications Alliance noted that it has conducted an analysis of the privacy-related complaints data generated by the TIO as a result of Communications Alliance's review of the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999). This research suggests that the TIO is classifying what actually are telemarketing related complaints as privacy complaints. Further, some of these complaints may be attributed incorrectly to the telemarketing activities of a supplier, when the unsolicited telemarketing activity is the action of an independent telemarketing agency. Communications Alliance submitted that, although the TIO recorded 2,718 complaints relating to privacy in 2004–05, it may be that reported privacy breaches in the telecommunications sector are not as prevalent as the TIO's statistics would suggest: Communications Alliance Ltd, *Submission PR 198*, 16 February 2007.

262 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 44, 48.

263 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [6.1]. It can also recommend the provision of compensation for amounts between $10,000 and $50,000: see *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [6.2].

264 The powers of the Privacy Commissioner to make determinations are discussed in Ch 49.

265 Australian Communications Authority, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [1.3]; Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, 9.

266 Australian Communications Authority, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [1.3].

267 Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, [1.7].

privacy regulators to 'ensure that privacy complaints are handled efficiently and to minimise confusion and costs for both individuals and organisations'.[268]

73.202 Although it is not a regulator, the Communications Alliance plays a key role in the regulation of the telecommunications sector. Membership of the Alliance is drawn from a cross-section of the communications industry, including service providers, vendors, consultants and suppliers as well as business and consumer groups. The Alliance develops and promotes compliance with industry codes. It has put in place a scheme that allows a carrier or carriage service provider to commit formally to comply with Communications Alliance Industry Codes. Part 6 of the *Telecommunications Act* provides that organisations such as Communications Alliance can create industry codes in relation to privacy for the telecommunications sector.

73.203 In DP 72, the ALRC noted that stakeholders had raised a range of issues concerning multiple bodies with responsibility for privacy in the telecommunications industry. Stakeholders noted that the overlapping complaints regime results in confusion and a loss of confidence by consumers in the ability of the telecommunications industry to handle their complaint; delay in the resolution of complaints; increased compliance costs for telecommunications providers; duplication of effort by regulators; and forum shopping. It was submitted that the regulatory roles of ACMA, the TIO and the OPC, as well as the Communications Alliance, should be clarified and relationships strengthened. Some stakeholders suggested that the OPC should be responsible for all telecommunications privacy matters, while others noted that the OPC does not have the resources or the expertise to deal with telecommunication privacy matters.[269]

73.204 The ALRC has concluded that there are advantages in having multiple bodies with responsibility for telecommunications privacy. Industry-specific regulators, such as ACMA and the TIO, play an important role as they provide industry expertise. Industry-specific regulators also reduce the volume of privacy complaints that would otherwise be made to the OPC, freeing the OPC's resources for other functions. Another potential benefit is peer review and the promotion of high standards of performance.

73.205 In the ALRC's view, however, the relationship between the various bodies with responsibility for telecommunications privacy needs to be clarified and strengthened. The ALRC has considered only the role of each of these bodies in relation to the regulation of privacy. The role and function of each of these bodies in the regulation of the telecommunication industry more broadly should be considered as part of the review recommended in Chapter 71.[270]

---

268 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159.

269 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [64.119]–[64.126].

270 Rec 71–2.

Memorandums of understanding

73.206 The Privacy Commissioner has entered into agreements with the New Zealand Privacy Commissioner and the Commonwealth Ombudsman that allow for greater cooperation between their respective offices when dealing with privacy-related complaints. In DP 72, the ALRC proposed that the OPC, TIO and ACMA should develop memorandums of understanding, addressing: the roles and functions of each of the bodies under the *Telecommunications Act*, *Spam Act*, *Do Not Call Register Act* and the *Privacy Act*; the exchange of relevant information and expertise between the bodies; and when a matter should be referred to, or received from, the bodies.[271]

Submissions and consultations

73.207 A large number of stakeholders supported this proposal.[272] Some stakeholders submitted that the arrangements outlined in the memorandums of understanding should be publicly available.[273] The Communications Alliance submitted that it should be a party to the memorandums of understanding.[274] Optus submitted that the OPC should have full responsibility for privacy regulation.[275]

ALRC's view

73.208 The OPC, TIO and ACMA should develop memorandums of understanding that address the roles and functions of each of the bodies relating to complaint handling under the *Telecommunications Act*, *Spam Act*, *Do Not Call Register Act* and the *Privacy Act.* Such agreements also should address the exchange of relevant information and expertise between the bodies.

73.209 As the regulator with expertise in privacy, the OPC should provide advice to the TIO in relation to the interpretation of the model UPPs, and to ACMA on whether a privacy issue is dealt with better under the *Privacy Act* or the *Telecommunications Act*. Conversely, given that the TIO and ACMA have expertise in telecommunications issues, they should assist the OPC when it is investigating a telecommunications-related privacy matter.

73.210 The ALRC does not recommend that the Communications Alliance should be a party to the memorandums of understanding because it is not a regulator and does not handle complaints. The Communications Alliance, however, should have a role in the

---

271 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–5.

272 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

273 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

274 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

275 Optus, *Submission PR 532*, 21 December 2007.

development of guidance and educational material on privacy in the telecommunications industry.[276]

Recommendation 73–8 The Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority should develop memorandums of understanding, addressing:

(a) the roles and functions of each of the bodies under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and *Privacy Act*;

(b) the exchange of relevant information and expertise between the bodies; and

(c) when a matter should be referred to, or received from, the bodies.

Complaint-handling policies

73.211 In DP 72, the ALRC proposed that the OPC prepare and publish a document setting out its complaint-handling policies and procedures,[277] and develop and publish enforcement guidelines.[278] The ALRC also proposed that these documents should set out the roles and functions of the OPC, TIO and ACMA under the *Telecommunications Act*, *Spam Act*, *Do Not Call Register Act* and *Privacy Act*; including when a matter will be referred to, or received from, the TIO and ACMA.[279] All stakeholders that addressed this issue supported the proposal.[280]

73.212 In Part F, the ALRC recommends that the OPC should develop and publish a document setting out its complaint-handling policies and procedures.[281] Consolidating this information into one document should increase the accessibility and transparency of the complaint-handling process, and provide a useful resource for agencies,

276 See Recs 73–10, 73–11.
277 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–8.
278 Ibid, Proposal 46–2.
279 Ibid, Proposal 64–6.
280 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007.
281 Rec 49–8.

organisations and individuals. The ALRC also recommends that the OPC should develop and publish enforcement guidelines.[282]

73.213 Both these documents should set out the roles and functions of the OPC, TIO and ACMA under the *Telecommunications Act*, *Spam Act*, *Do Not Call Register Act* and *Privacy Act*; including when a matter will be referred to, or received from, the TIO and ACMA. The TIO and ACMA also should develop and publish a complaint-handling policy and enforcement guidelines.

Recommendation 73–9 The document setting out the Office of the Privacy Commissioner's complaint-handling policies and procedures (see Recommendation 49–8), and its enforcement guidelines (see Recommendation 50–3) should address:

(a) the roles and functions of the Office of the Privacy Commissioner, Telecommunications Industry Ombudsman and the Australian Communications and Media Authority under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and *Privacy Act*; and

(b) when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.

Guidance

73.214 In DP 72, the ALRC proposed that the OPC, in consultation with ACMA, Communications Alliance and the TIO, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should:

- outline the interaction between the *Privacy Act*, *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*;
- provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and
- outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.[283]

282 Rec 50–4.

283 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–7.

Submissions and consultations

73.215 A number of stakeholders supported this proposal.[284] The DBCDE submitted that there appears to be considerable merit in providing greater guidance on the interaction between the relevant Acts, particularly the exemption and consent arrangements. The Department noted, however, that it may be more appropriate for ACMA to have primary carriage of this responsibility, in consultation with the DBCDE. The Department's view was based on ACMA's expertise in regulation of the telecommunications industry and the Department's responsibility for telecommunications policy.[285]

73.216 One stakeholder noted, however, that she had concerns about 'consent as it applies in various contexts' being covered in guidance and not legislation, and that the ALRC's proposal mentioned the involvement of Communications Alliance, but not privacy advocates or consumer organisations.[286]

ALRC's view

73.217 Since the deregistration of the Australian Communications Industry Forum *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, there is little published guidance on information privacy in the telecommunications industry.

73.218 Submissions to the OPC Review and the current Inquiry indicate that telecommunications providers, regulators and individuals would benefit from the development of such a document, particularly in relation to the interaction between the *Privacy Act* and other legislation that deals with telecommunications privacy issues.

73.219 The guidance should outline the interaction between the *Privacy Act*, *Telecommunications Act*, *Spam Act*, and *Do Not Call Register Act* and include advice on the operation of the exceptions, and on what is required to obtain an individual's consent under each Act. Issues related to exceptions and consent under telecommunications legislation are discussed in more detail above and in Chapter 72.

73.220 All bodies with responsibility for telecommunications privacy should be involved in the development of this guidance. The ALRC has concluded, however, that ACMA should have primary responsibility for the development of this advice, as the regulatory body with expertise in the regulation of the telecommunications industry.

---

284 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

285 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

286 I Graham, *Submission PR 427*, 9 December 2007.

The guidance should be developed in consultation with relevant stakeholders, including the OPC, TIO, DBCDE, Communications Alliance, privacy advocates and consumer groups, and bodies that represent the direct marketing industry.

Recommendation 73–10 The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should:

(a) outline the interaction between the *Privacy Act*, *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth);

(b) provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and

(c) outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act*, *Spam Act* and *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.

Educational material

73.221 In DP 72, the ALRC proposed that the OPC, in consultation with the AGD, ACMA, the Office of the Commonwealth Ombudsman, the IGIS and the TIO, should develop and publish educational material that addresses: the rules regulating privacy in the telecommunications industry; the various bodies that are able to deal with a complaint in relation to privacy in the telecommunications industry; and how to make a complaint to those bodies.[287]

Submissions and consultations

73.222 All stakeholders that addressed this issue supported the proposal.[288] The DBCDE supported the proposal but noted that it may be more appropriate for ACMA to have primary carriage of this responsibility, in consultation with the DBCDE. In the DBCDE's view, ACMA may be better suited to this role as it has expertise in regard to regulation of the telecommunications industry.[289]

---

287 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 64–8.

288 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007.

289 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

ALRC's view

73.223 The ALRC notes that the TIO publishes a number of 'Position Statements' designed to inform the public about a range of telecommunications issues, including privacy. ACMA also publishes on its website some material on Part 13 of the *Telecommunications Act*. There is little information about the operation of the *Telecommunications (Interception and Access) Act* on the website of the AGD.

73.224 It is important that individuals are aware of the obligations of agencies and organisations under telecommunications privacy laws, and know how to seek redress for a breach of those obligations. The ALRC recommends that ACMA, in consultation with relevant stakeholders, should develop and publish educational material that addresses: the rules regulating privacy in the telecommunications industry; the various bodies that are able to deal with a telecommunications privacy complaint; and how to make a complaint to those bodies. These stakeholders would include the OPC, TIO, DBCDE, Communications Alliance, privacy advocates and consumer groups.

73.225 These educational materials also should address agencies' and organisations' obligations under the *Telecommunications (Interception and Access) Act*. ACMA should consult with the bodies with responsibility for the administration and oversight of that legislation—namely, the AGD, the IGIS, and the Commonwealth Ombudsman.

Recommendation 73–11 The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish educational material that addresses the:

(a) rules regulating privacy in the telecommunications industry; and

(b) various bodies that are able to deal with a telecommunications privacy complaint, and how to make a complaint to those bodies.

Part K

Protecting a Right to Personal Privacy

74. Protecting a Right to Personal Privacy

Contents

Introduction

74.1 A tort of invasion of privacy has found legislative expression in some jurisdictions in the United States and Canada since the 1970s. While the courts in the United Kingdom (UK) do not recognise such a tort by that name, in practice, the equitable action for breach of confidence has been used to address the misuse of private information. The New Zealand courts have recognised the existence of a common law tort of privacy. In Australia, no jurisdiction has enshrined in legislation a cause of action for invasion of privacy; however, the door to the development of such a cause of action at common law has been left open by the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (*Lenah Game Meats*).[1] To

1 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

date, two lower courts have held that such a cause of action is part of the common law of Australia.[2]

74.2 The development of a tort of invasion of privacy by the common law courts may result in piecemeal and fragmented privacy protection, with some jurisdictions prepared to take an active role in the development of the tort and others waiting for further guidance from the High Court. In the context of privacy protection this is problematic. It may be difficult for individuals and organisations (such as media outlets) to assess the effect of the law on their operations and to implement appropriate policies to minimise their potential liability if the common law is developing at different rates and with variations from state to state (as was the case for many years with the law of defamation). Some courts also may choose to adopt the 'breach of confidence' approach based on case law in the UK, which would result in further inconsistency.

74.3 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that, to ensure consistent privacy protection in this area, a cause of action for a serious invasion of privacy should be recognised by the legislature in Australia.[3] It was also noted that, as part of its review of privacy laws in New South Wales, the New South Wales Law Reform Commission (NSWLRC) is looking at the desirability of introducing a statutory tort of privacy in that state. In May 2007, the NSWLRC released Consultation Paper 1, *Invasion of Privacy* (NSWLRC CP 1), which is discussed in detail below. In DP 72, the ALRC generally agreed with the proposals for reform put forward in NSWLRC CP 1.

74.4 In DP 72, the ALRC confirmed that, in an effort to ensure uniform development in this important area of law, the NSWLRC would take primary responsibility for the formulation of proposals for reform. With the consent of those consulted or making a submission, consultation notes and submissions to the ALRC Inquiry were shared with the NSWLRC.

74.5 This Report has been published before the NSWLRC has finalised its report on this issue. The ALRC necessarily has made its own recommendations in relation to the possible enactment in federal law of a cause of action for serious invasion of privacy. The ALRC remains committed to the view that uniform development in this area of law would be desirable. The views of the ALRC in this Report, however, should not be taken as the final views of the NSWLRC.

---

2 *Grosse v Purvis* (2003) Aust Torts Reports 81–706; *Doe v Australian Broadcasting Corporation* [2007] VCC 281. These cases are discussed below.

3 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 5–1 to 5–7.

74.6 In this chapter, the ALRC outlines:

- an overview of developments in the law on this issue in Australia and elsewhere;
- NSWLRC CP 1, with particular emphasis on the impact federally of the issues discussed in that consultation paper;
- the submissions and consultations to this Inquiry; and
- the ALRC's recommendations for the introduction of a statutory cause of action for a serious invasion of privacy.

Background

Previous ALRC reports

74.7 The ALRC first considered the protection of privacy through tort law in *Unfair Publication: Defamation and Privacy*.[4] After reviewing the case law relating to privacy in Australia, proposals by academics and state legislatures aimed at protecting privacy, and approaches to the protection of privacy adopted in overseas jurisdictions, the ALRC proposed a tort of 'unfair publication'. The tort was designed to protect from publication the details of individuals' sensitive private facts relating to their home life, private behaviour, health, and personal and family relationships. It was designed to protect against the appropriation for commercial or political purposes of a person's name, identity, reputation or likeness.[5]

74.8 Significantly, the ALRC intended that the scope of the tort would be limited to the publication of 'sensitive' facts.[6] The publication would have to cause distress, embarrassment or annoyance to a person in the position of that individual for an action in tort to lie.[7] For example, the ALRC suggested that the publication, without consent, of a photograph taken in a private place could give rise to an action in the tort of unfair publication where the photograph related to the individual's home life, private behaviour, health, or personal and family relationships.[8]

74.9 The ALRC also recommended that an action in tort be available to a person whose name, identity or likeness was published by another person (Y) in circumstances where Y had not obtained the consent of the first person (X), and the publication was for Y's own benefit with the intent to exploit X's name, identity or likeness. The

4 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979).
5 Ibid, [250].
6 Sensitive facts were defined as facts relating to a person's individual relationships, health, home, family and private life: Ibid, [236].
7 Ibid, [236].
8 Ibid, [240].

ALRC confined its recommendation on this issue to matters published for commercial purposes or candidature of office.[9]

74.10 In its later report, *Privacy* (ALRC 22), the ALRC declined to recommend the creation of a general tort of invasion of privacy. In the ALRC's view at that time, 'such a tort would be too vague and nebulous'.[10]

Privacy Act 1988 (Cth)

74.11 During the passage through Parliament of the Privacy Bill 1988 (Cth), the Senate proposed an amendment to the Bill to provide for an action for breach of privacy. The proposed amendment provided that 'interference with the privacy of an individual taking place after the commencement of this Act shall give rise to an action at the suit of the individual for breach of privacy'.[11] The remedies that the Federal Court or the Supreme Court of a state or territory could award under such an action also were stipulated.[12]

74.12 The Senate's proposed amendment was narrower than the general tort of invasion of privacy that the ALRC declined to proceed with in ALRC 22. The proposed statutory cause of action only would lie 'against an agency or a tax file number recipient or both'.[13] The House of Representatives rejected the proposed amendment.[14]

Article 17 of the ICCPR

74.13 As has been noted elsewhere in this Report,[15] on 13 August 1980 the Australian Government ratified the *International Covenant on Civil and Political Rights* (ICCPR). Article 17 of the ICCPR states:

> 1. No person shall be subjected to arbitrary or unlawful interferences with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[16]

---

9 Ibid, [250].

10 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1081].

11 Parliament of Australia—Senate, *Schedule of the Amendments Made by the Senate to Privacy Bill 1988 (1987–88)* (1988), cl 63A.

12 Ibid, cl 63C. These remedies included damages; injunctions; an order to deliver to the claimant any documents brought into existence in the course of the interference with privacy; or any other order that the court considered just.

13 Ibid, cl 63B.

14 Parliament of Australia—House or Representatives, *Schedule of the Amendments Made by the Senate to the Privacy Bill 1988 to which the House of Representatives has Disagreed* (1988).

15 See Chs 1, 2, 3, 5.

16 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

74.14 In 1988, the Office of the United Nations (UN) High Commissioner for Human Rights released General Comment Number 16, which discussed how the UN interprets art 17 and how it should be promoted through domestic law. It is noted in the General Comment that art 17 should protect a nation's citizens against all interferences and attacks on privacy, family, home or correspondence, 'whether they emanate from State authorities or from natural or legal persons'.[17] To this end, all member states are required 'to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right'.[18] Furthermore, 'state parties are under a duty themselves not to engage in interferences inconsistent with art 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons'.[19]

74.15 As noted in Chapter 2, the Preamble to the *Privacy Act* makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the ICCPR. The *Privacy Act*, however, is concerned with information privacy only, and therefore is not a full implementation in domestic law of the meaning of art 17. The ACT and Victoria are the only Australian jurisdictions that currently possess a bill of rights.[20] Section 12 of the *Human Rights Act 2004* (ACT) and s 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) recognise a right to privacy and reputation, both stating that:

> Everyone has the right—
>
> (a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and
>
> (b) not to have his or her reputation unlawfully attacked.

Right to personal privacy—developments in Australia and elsewhere

74.16 Common law and legislative developments in Australia and other comparable overseas jurisdictions cast light on the policy choices available for reform in this area. Of particular interest are the statutory expressions of the tort of invasion of privacy in the United States, some of the provinces of Canada[21] and the Privacy Bill considered by the Irish Parliament.[22] Common law developments—in the UK, New Zealand and

---

17 United Nations Office of the High Commissioner for Human Rights, *General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art 17)* (1988), [1].

18 Ibid, [1].

19 Ibid, [9].

20 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25; *Charter of Human Rights and Responsibilities Act 2006* (Vic).

21 *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act* CCSM s P125 (Manitoba); *Privacy Act 1978* RSS c P–24 (Saskatchewan); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador).

22 Privacy Bill 2006 (Ireland).

Australia—of the test to determine what is considered 'private' for the purpose of determining liability for a breach of privacy are also of interest.

Statutory models

United States

74.17 In 1960, Professor William Prosser surveyed American case law and found not one tort protecting privacy interests but 'a complex of four'.[23] The *Second Restatement of the Law, Torts*[24] has adopted Prosser's classification and provides for privacy tort protection where:

> 1 One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person;
>
> 2 One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy;
>
> 3 One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public;
>
> 4 One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[25]

74.18 The privacy torts are subject to the same defences that apply in the United States to defamation.[26] Such defences include: an absolute parliamentary and court privilege; consent; and conditional privileges for other activities, such as reporting public proceedings and reasonable investigation of a claim against a defendant.[27]

74.19 The privacy torts have proved to be of limited effect, due in no small part to the existence of a constitutionally entrenched right to a free press. If the subject is newsworthy, and the newsworthy event occurs in a public place, privacy protection tends to take a back seat to the First Amendment protection of freedom of the press.[28] The concept of 'newsworthy' in the United States appears to be broader than the

---

23 R Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 389.

24 The Restatements of the Law are expositions on the law on specific subjects (based on court decisions) published by the American Law Institute.

25 *Restatement of the Law, 2nd, Torts 1977* (US) §§ 652B, 652C, 652D, 652E.

26 Ibid §§ 652F–652H.

27 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 343.

28 S Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349.

concept of 'public interest'—and, in particular, the right to freedom of expression—discussed below, applied by the UK courts in privacy cases.

74.20 The State of California has attempted to provide some additional protection, in particular for celebrities, through the enactment of a cause of action for physical invasion of privacy. This applies

> when the defendant knowingly enters on to the land of another without permission or otherwise commits a trespass in order to physically invade the privacy of the plaintiff with the intent to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity and the physical invasion occurs in a manner that is offensive to a reasonable person.[29]

74.21 To address the problems associated with an evolving technological environment, § 1708.8 of the *California Civil Code* also establishes an action for constructive invasion of privacy when

> the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or other familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.[30]

74.22 The legislation has been in force since 1998,[31] and the provision's teeth are found in the penalties that apply for committing the invasion, constructive invasion or assault. The penalties include up to three times the amount of general and special damages ('treble damages') proximately caused by the invasion, constructive invasion or assault; punitive damages; and possible forfeiture of any proceeds or consideration obtained.[32] Those that direct, solicit, actually induce or cause another person to commit such an assault may also be liable.[33] Whether the legislation survives a constitutional challenge remains to be seen.[34]

---

29 *California Civil Code* § 1708.8(a).

30 Ibid § 1708.8(b).

31 The current § 1708.8(c) was enacted in 2005: S Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349, 1353.

32 *California Civil Code* § 1708.8(d). If an assault is committed with the intent to capture the visual image, sound recording, or other physical impression of the plaintiff, the penalties in § 17808.8(d)–(h) also apply: *California Civil Code* § 1708.8(c).

33 *California Civil Code* § 1708.8(e).

34 S Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349, 1353–1355.

Canada

74.23 An individual's right to privacy has received statutory protection in four provinces in Canada.[35] Generally, the legislation provides that 'it is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person'.[36] The legislation also stipulates a number of general defences, including consent, exercise of a lawful right of defence of person or property, acts or conduct authorised or required by law, privilege and fair comment on a matter of public interest.[37] Remedies include damages, an injunction, an account for profits and an order for the delivery up of material.[38]

74.24 While the *Canadian Charter of Rights and Freedoms 1982*[39] does not specifically guarantee a right to privacy, the Supreme Court of Canada has interpreted the right in s 8 to be secure against unreasonable search and seizure to include a reasonable expectation of privacy in relation to governmental acts.[40] The province of Quebec has guaranteed 'a right to respect for … personal life' in the Quebec *Charter of Human Rights and Freedoms*.[41]

Ireland

74.25 In 2006, the Irish Parliament considered the Privacy Bill 2006 which would have established a 'tort of invasion of privacy' in Irish law. Under the Bill, the tort would have been actionable without proof of damage, but limited to deliberate and intentional conduct, without lawful authority.[42] The Bill stated that a person is entitled to privacy that is 'reasonable in all the circumstances having regard to the rights of others and to the requirements of public order, public morality and the common good'.[43]

---

35 *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act* CCSM s P125 (Manitoba); *Privacy Act 1978* RSS c P–24 (Saskatchewan); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador).

36 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 2. See also *Privacy Act 1996* RSBC c 373 (British Columbia) s 1(1); *Privacy Act* CCSM s P125 (Manitoba) s 2(1); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 3(1). The British Columbia legislation differs from the statutes in force in the other provinces in that it also protects the unauthorised use of the name or portrait of another: *Privacy Act 1996* RSBC c 373 (British Columbia) s 3.

37 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 4; *Privacy Act 1996* RSBC c 373 (British Columbia) s 2(2), (3) and (4); *Privacy Act* CCSM s P125 (Manitoba) s 5; *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 5.

38 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 7; *Privacy Act* CCSM s P125 (Manitoba) s 4(1); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 6(1). For an analysis of the impact of the legislation, see S Chester, J Murphy and E Robb, 'Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?' (2003) 27 *Advocates Quarterly* 357.

39 Enacted as Schedule B to the *Canada Act 1982* c 11 (UK), which came into force on 17 April 1982.

40 *R v Dyment* [1988] 2 SCR 417, 426. See also *Godbout v Longueuil (City)* [1997] 3 SCR 844, 913 (s 8 of the *Canadian Charter of Rights and Freedoms* guarantees a sphere of individual autonomy for all decisions relating to 'choices that are of a fundamentally private or inherently personal nature').

41 *Charter of Human Rights and Freedoms* RSQ c–12 (Quebec) s 5. Generally, see the discussion of privacy law in Canada in *Hosking v Runting* [2005] 1 NZLR 1, [60]–[65].

42 Privacy Bill 2006 (Ireland), cl 2(1), 2(2).

43 Ibid, cl 3(1).

74.26 As noted below, the Bill was criticised by journalists as limiting the right to freedom of the press and inhibiting investigative journalism.[44] In 2007, it was reported that the Irish Government had decided not to proceed with the Bill.[45]

Common law developments

United Kingdom

74.27 The developments in the UK have been influenced in recent years by the *European Convention on Human Rights* (ECHR) and the *Human Rights Act 1998* (UK) (HRA 1998). The ECHR contains a right to private and family life, home and correspondence in art 8.[46] The HRA 1998 incorporates (to some extent) the ECHR into the domestic law of the UK.[47] The HRA 1998 came into force in October 2000.[48]

74.28 There is no freestanding right to privacy in the UK. The courts repeatedly have stated that 'English law knows no common law tort of invasion of privacy'.[49] Instead, the cause of action for breach of confidence has been extended to encompass misuse or wrongful dissemination of private information.[50] Extensive expansion of the law in this area has occurred in recent years.

74.29 The formulation of the cause of action for breach of confidence was set out in *Coco v A N Clark (Engineers) Ltd*.[51] To establish the cause of action, at that time: the information must have had the necessary quality of confidence; the information must have been imparted in circumstances giving rise to an obligation of confidence; and there must have been unauthorised use of that information to the detriment of the party communicating it.

---

44 See New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [3.61]–[3.63].

45 F Sheanan 'New Libel Law is Top Priority as Privacy Bill is Shelved', *Independent* (online), 12 November 2007, <www.independent.ie>.

46 Article 8(1) provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. Article 8(2) provides that 'there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

47 Section 6 of the *Human Rights Act 1998* (UK) requires public authorities, including courts, to act in accordance with the *European Convention on Human Rights*. The domestic courts are also given the task of reading domestic legislation in line with the *European Convention on Human Rights*, via s 3. When interpreting Convention rights the courts must take into account Strasbourg jurisprudence: *Human Rights Act 1998* (UK) s 2.

48 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 10 December 1948, Council of Europe, ETS No 005, (entered into force generally on 3 September 1953). The Convention was implemented by the *Human Rights Act 1998* (UK).

49 *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920, [272]. See also *Wainwright v Home Office* [2004] 2 AC 406.

50 *Campbell v MGN Ltd* [2004] 2 AC 457; B McDonald, 'Privacy, Princesses, and Paparazzi' (2005–2006) 50 *New York Law School Law Review* 205, 232. See also *Hosking v Runting* [2005] 1 NZLR 1, [23]–[53].

51 Coco v AN Clark (Engineers) Ltd [1969] RPC 41.

74.30 The evolution of the cause of action for breach of confidence was summarised by Lord Phillips MR in *Douglas v Hello!*

> Megarry J in *Coco v A N Clark* identified two requirements for the creation of a duty of confidence. The first was that the information should be confidential in nature and the second was that it should have been imparted in circumstances importing a duty of confidence. As we have seen, it is now recognised that the second requirement is not necessary if it is plain that the information is confidential, and for the adjective 'confidential' one can substitute the word 'private'. What is the nature of 'private information'? It seems to us that it must include information that is personal to the person who possesses it and that he does not intend shall be imparted to the general public. The nature of the information, or the form in which it is kept, may suffice to make it plain that that the information satisfies these criteria.[52]

74.31 In *Ash v McKennitt*, the English Court of Appeal recognised that a

> feeling of discomfort arises from the action for breach of *confidence* being employed where there was no pre-existing relationship of confidence between the parties, but the 'confidence' arose from the defendant having acquired by unlawful or surreptitious means information that he should have known he was not free to use …[53]

74.32 The court went on to note that, 'at least the verbal difficulty … has been avoided by the rechristening of the tort as misuse of private information: per Lord Nicholls of Birkenhead in *Campbell*'.[54]

74.33 The House of Lords decision in *Campbell v MGN Ltd* is the leading authority on the scope of what subsequently has been termed, in the Court of Appeal hearing in *Douglas*, as the 'the cause of action formally described as breach of confidence'.[55]

74.34 Model Naomi Campbell brought proceedings in breach of confidence against Mirror Group Newspapers in relation to a newspaper article which stated that she was a drug addict and that she was attending Narcotics Anonymous. The article was accompanied by a photograph of Campbell on a public street outside a Narcotics Anonymous premises. Campbell succeeded in her claim at first instance, however, this was overturned in the Court of Appeal. The case was taken to the House of Lords.

74.35 Campbell conceded early on in proceedings that the newspaper was entitled to publish the fact that she had a drug problem and that she was receiving treatment. She conceded this aspect of the publication because she had previously asserted the fact that, unlike other models, she did not abuse drugs and, therefore, disclosure was in the public interest.

74.36 The House of Lords was left to consider whether Campbell's treatment, the fact that she was attending Narcotics Anonymous and the photograph constituted an

---

52 *Douglas v Hello! Ltd* [2005] EWCA Civ 595.
53 *Ash v McKennitt* [2007] 3 WLR 194, [8] (emphasis in original).
54 Ibid, [8].
55 *Douglas v Hello! Ltd* [2005] EWCA Civ 595, [53].

invasion of her privacy. The House of Lords found, by a 3:2 majority, that those features did constitute an invasion of her privacy. Reporting that her treatment was being provided by Narcotics Anonymous and the details of that treatment 'went significantly beyond the publication of the fact that she was receiving therapy or that she was engaged in a course of therapy with [Narcotics Anonymous]'.[56]

European Convention on Human Rights

74.37 Developments in the UK regarding an action for breach of privacy must now be discussed with reference to the human rights legislation in force in the European Union. The ECHR came into force in the UK in October 2000.[57] Since that time, the courts in the UK have been influenced by art 8 of the Convention,[58] and by the Strasbourg jurisprudence interpreting this article.[59]

74.38 When analysing whether the elements of the tort have been established in a case of unlawful publication of private information (which, to date, constitutes the majority of the case law in the UK), the court engages in a two-part balancing exercise. The court first ascertains whether the information is private 'in the sense that it is in principle protected by article 8'. If the answer is 'yes', the court then asks: 'in all the circumstances, must the interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by article 10'? [60]

74.39 Professor Gavin Phillipson has summarised the development in *Campbell* as follows:

> The House recognised that the first port of call in determining whether there are facts worthy of protection should be the Article 8 case law and, secondly, that the test of high offensiveness was therefore not to be used as a threshold test, which had to be satisfied in all cases, but rather only as a tie-breaker, to determine marginal or doubtful cases and to be used to help determine the weight or seriousness of the privacy interest when balancing it against the competing interest in publication.[61]

74.40 The courts in the UK have avoided setting too high a bar when determining what 'private' means within the context of art 8. When considering the first limb of the

---

56 *Campbell v MGN Ltd (No 2)* [2005] 4 All ER 793, [117].

57 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 10 December 1948, Council of Europe, ETS No 005, (entered into force generally on 3 September 1953). The Convention was implemented by the *Human Rights Act 1998* (UK).

58 Article 8(1) provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'.

59 *Ash v McKennitt* [2007] 3 WLR 194, [11].

60 Ibid, [11].

61 G Phillipson, 'The 'Right' of Privacy in England and Strasbourg Compared' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 184, 193.

test, the person alleging a breach of art 8 must establish that interference with private life was of 'some seriousness' before the article is engaged.[62]

74.41 It is unclear whether 'some seriousness' equates to, or is lower than, the standard of disclosure that is 'highly offensive to a reasonable person of ordinary sensibilities', propounded in cases such as *Lenah Game Meats*.[63] In *Campbell*, Nicholls LJ warned that the 'highly offensive' formulation

> should be used with care for two reasons. First, the 'highly offensive' phrase is suggestive of a stricter test of private information than a reasonable expectation of privacy. Second, the 'highly offensive' formulation can all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which publication was a matter of proper public concern. This could be a recipe for confusion. [64]

74.42 Hope LJ noted that the threshold test is 'what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity'.[65] Baroness Hale LJ suggested a similar formulation.[66]

74.43 Once the information is identified as 'private', the court must then 'balance the claimant's interest in keeping the information private against the countervailing interest of the recipient in publishing it'.[67] This balancing test is contextual—that is, determined by reference to the facts of the particular case. The principles formulated by the trial judge in *McKennitt v Ash*,[68] and endorsed by the English Court of Appeal, to determine the second limb of the test are:

> i) Neither article [8 nor art 10 of the ECHR] has as such precedence over the other.
>
> ii) Where conflict arises between the values under Articles 8 and 10, an 'intense focus' is necessary upon the comparative importance of the specific rights being claimed in the individual case.
>
> iii) The court must take into account the justifications for interfering with or restricting each right.
>
> iv) So too, the proportionality test must be applied to each.[69]

74.44 Shortly after the decision in *Campbell*, the European Court of Human Rights decided *Von Hannover v Germany*,[70] which concerned a claim brought by

---

62 *Ash v McKennitt* [2007] 3 WLR 194, [12]; *M v Secretary of State for Work and Pensions* [2006] 2 AC 91, [83].
63 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.
64 *Campbell v MGN Ltd* [2004] 2 AC 457, [22].
65 Ibid, [99].
66 Ibid, [136].
67 Ibid, [137].
68 *McKennitt v Ash* [2005] EMLR 10.
69 *Ash v McKennitt* [2007] 3 WLR 194, [46].
70 *Von Hannover v Germany* [2004] ECHR 294.

Princess Caroline of Monaco on the basis that certain decisions of the German courts had infringed her right under art 8 to respect for her private life.

74.45 A number of photographs of Princess Caroline had been published in German magazines. The photographs consisted of images of the Princess with her children; with a male friend at a restaurant; on holiday and engaged in sporting activities with her husband; and at the Monte Carlo Beach Club, where she was dressed in a swimsuit. One of the beach club images showed the Princess falling over.

74.46 The Princess brought a number of claims for injunction against the media in the German courts. The German Federal Court granted her relief in respect of the restaurant photographs and photographs of the Princess and her children. The European Court of Human Rights, therefore, was asked to uphold her right to privacy in relation to the photographs of the Princess on holiday, engaged in sporting activities with her husband and at the Monte Carlo Beach Club.

74.47 In *Von Hannover*, the European Court of Human Rights established the benchmark from which an analysis of the application of art 8 must proceed. The Court recognised the 'fundamental importance of protecting private life from the point of view of the development of every human being's personality'.[71] The Court noted that the protection 'extends beyond the private family circle and also includes a social dimension … anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection of and respect for their private life'.[72]

74.48 It is clear from the reasoning in *Von Hannover* that the Court took into account—to use the words found in the Terms of Reference for this Inquiry[73]—'the need of individuals for privacy in an evolving technological environment'. The Court stressed the fact that 'increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data'.[74]

74.49 The *Von Hannover* case suggests that the obligation to respect private life does not encapsulate merely activities conducted in private or sensitive events occurring in public. The obligation also extends to relatively ordinary daily activities occurring in public places. This is quite different from the reasoning of the English Court of Appeal in *Campbell*. In that case, Lady Hale found that the mere fact that the photography is covert does not make the act recorded private.

---

71 Ibid, [69].
72 Ibid, [69].
73 The Terms of Reference are reproduced at the beginning of this Report.
74 *Von Hannover v Germany* [2004] ECHR 294, [70].

> The activity photographed must be private. If … she pops out to the shops for a bottle of milk … there is nothing essentially private about that information nor can it be expected to damage her private life.[75]

74.50 The extent of 'private life', therefore, remains unclear following the *Von Hannover* decision.

74.51 Phillipson has identified two potential interpretations of *Von Hannover*. The 'absolutist' interpretation is

> the view that any publication of an unauthorised photograph specifically taken of a particular person engaged in an everyday activity outside their official duties will involve a *prima facie* violation of art 8.[76]

74.52 Recognising that the courts may be inclined to read down *Von Hannover*, however, he also identified a more restrictive reading of the judgment, which he thought that the courts may adopt to 'reconcile that decision [*Von Hannover*] with *Campbell*'. The narrow interpretation claims that two elements were essential for the finding that art 8 was engaged in *Von Hannover*. Those two elements were: (a) the fact that the pictures relate to the Princess's everyday life, not her official functions; and (b) the constant intrusion that persistent photographing represents.[77]

74.53 This interpretation limits the scope of *Von Hannover* to cases where an element of harassment is present. The narrow interpretation received some endorsement in *John v Associated Newspapers*,[78] but was dismissed in *McKennitt v Ash*[79] and in the decision at first instance in *Murray v Express Newspapers*.[80]

74.54 Despite rejecting the narrow approach, the courts arguably have adopted a middle ground in cases such as *McKennitt v Ash*.[81] As noted above, in *McKennitt v Ash*, the Court of Appeal held that the person alleging a breach of art 8 must establish that interference with private life was of 'some seriousness' before art 8 is engaged.[82] This contradicts the principle underpinning *Von Hannover*, which, on an 'absolutist' reading of the judgment, leaves no scope for a test of 'seriousness'. In *Murray*, Patten J held that 'even after *Von-Hannover* there remains … an area of routine activity which when conducted in a public place carries no guarantee of privacy'.[83]

---

75 *Campbell v MGN Ltd* [2004] 2 AC 457, [154].

76 G Phillipson, 'The 'Right' of Privacy in England and Strasbourg Compared' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 184. The same argument is also made in H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (2006), ch 13.

77 Ibid, 227.

78 *John v Associated Newspapers* [2006] EMLR 722.

79 *Ash v McKennitt* [2006] EWCA Civ 1714, [41-42].

80 *Murray v Express Newspapers PLC* [2007] EWHC 1908.

81 Ibid.

82 *Ash v McKennitt* [2006] EWCA Civ 1714; See also *M v Secretary of State for Work and Pensions* [2006] 2 AC 91, [83].

83 *Murray v Express Newspapers PLC* [2007] EWHC 1908.

74.55 In *Murray*, Murray—who is also known as JK Rowling (the author of the *Harry Potter* books)—and her husband sued a photo agency on behalf of their 18 month old son. The agency's photographer took a covert photograph of the couple and their son on a street in Edinburgh. The photograph, which was published in a newspaper, clearly showed the son's face. Rowling and her husband claimed that the photograph breached their son's right to privacy, and that its publication was a misuse of private information.

74.56 In dismissing the case before trial, Patten J stated:

> If a simple walk down the street qualifies for protection then it is difficult to see what would not. For most people who are not public figures in the sense of being politicians or the like, there will be virtually no aspect of their life which cannot be characterised as private. Similarly, even celebrities would be able to confine unauthorised photography to the occasions on which they were at a concert, film premiere or some similar function.[84]

74.57 In the subsequent appeal, the Court of Appeal found that Patten J had incorrectly taken the view that the Murrays had sought, through an action in the name of their son, to establish a right to personal privacy for themselves and their family when engaged in ordinary family activities.[85] The Court of Appeal stated the child had a right to privacy distinct from that of his parents. As the appeal was against an order striking out the action, the Court of Appeal was not required to analyse the difference between *Von Hannover* and the UK cases in any detail. It did, however, make some comment as to when a reasonable expectation of privacy could arise.

> We do not share the predisposition identified by the judge … that routine acts such as a visit to a shop or a ride on a bus should not attract any reasonable expectation of privacy. All depends on the circumstances.[86]

74.58 In coming to this view, the Court of Appeal echoed some of the reasoning in *Von Hannover* by focusing on the intrusive nature of media attention on celebrities.

> It seems to us, that, subject to the facts of the particular case, the law should indeed protect children from intrusive media attention, at any rate to the extent of holding that a child has a reasonable expectation that he or she will not be targeted in order to obtain photographs for publication which the person who took or procured the taking of the photographs knew would be objected to on behalf of the child.[87]

New Zealand

74.59 In *Hosking v Runting*, a majority of the New Zealand Court of Appeal held that the tort of invasion of privacy should be recognised as part of the common law of New

---

84 Ibid, [65].
85 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, [14].
86 Ibid, [56].
87 Ibid, [57].

Zealand.[88] While the majority stressed that 'the cause of action will evolve through future decisions as courts assess the nature and impact of particular circumstances',[89] the Court was prepared to extend tort protection to wrongful publicity given to private lives. The Court of Appeal was influenced by the third formulation of the United States privacy tort,[90] holding that:

> there are two fundamental requirements for a successful claim for interference with privacy:
>
> 1 The existence of facts in respect of which there is a reasonable expectation of privacy; and
>
> 2 Publicity given to those private facts that would be considered highly offensive to an objective reasonable person.[91]

74.60 In the recent case of *Rogers v TVNZ*, the Court of Appeal considered whether a videotaped confession for trial (which TVNZ proposed to broadcast) could meet the test of a reasonable expectation of privacy. The court found that even though the tape was not inherently 'private', it could be considered to have been private outside its use in the courtroom. The court considered, however, that its privacy value was at the 'low end of the scale', which would impact on the later balancing of the right to privacy against other rights in favour of publishing the material.[92] In this case, those other rights were considered to be freedom of expression and open justice. The matter was sent back to the lower courts for substantive hearing.

Australia

74.61 Prior to 2001, the major obstacle to the recognition in Australia of a common law right to privacy was the 1937 High Court decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*.[93] In a subsequent decision, the High Court in *Lenah Game Meats* indicated clearly that the decision in *Victoria Park* 'does not stand in the path of the development of … a cause of action [for invasion of privacy]'.[94] The elements of such a cause of action—and whether the cause of action is to be left to the

---

88 For a detailed discussion of *Hosking v Runting* [2005] 1 NZLR 1, see D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 352–357.

89 *Hosking v Runting* [2005] 1 NZLR 1, [118].

90 Ibid, [118]. The third formulation is outlined above.

91 Ibid, [117].

92 *Rogers v TVNZ* [2007] NZSC 91, [59].

93 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479. See discussion in D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 341; Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [223].

94 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [107] (per Gummow and Hayne JJ, with whom Gaudron J agreed). See also Ibid, [187] (per Kirby J); [313]–[320] (per Callinan J). For a detailed analysis of the case, see G Taylor and D Wright, 'Australian Broadcasting Corporation v Lenah Game Meats: Privacy, Injunctions and Possums: An Analysis of the Court's Decision' (2002) 26 *Melbourne University Law Review* 707.

common law tradition of incremental development or provided for in legislation—remain open questions.[95]

74.62 Since then, two Australian cases have recognised expressly a common law right of action for invasion of privacy. In the 2003 Queensland District Court decision in *Grosse v Purvis*, Skoien SDCJ awarded aggravated compensatory damages and exemplary damages to the plaintiff for the defendant's breach of the plaintiff's privacy.[96] After noting that the High Court in *Lenah Game Meats* had removed the barrier the *Victoria Park* case posed to any party attempting to rely on a tort of invasion of privacy, his Honour took what he viewed as 'a logical and desirable step' and recognised 'a civil action for damages based on the actionable right of an individual person to privacy'.[97]

74.63 While emphasising that 'it is not my task nor my intent to state the limits of the cause of action nor any special defences other than is necessary for the purposes of this case', Skoien SDCJ enumerated the essential elements of the cause of action:

> 1 a willed act by the defendant;
>
> 2 which intrudes upon the privacy or seclusion of the plaintiff;
>
> 3 in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities; and
>
> 4 which causes the plaintiff detriment in the form of mental, physiological or emotional harm or distress, or which prevents or hinders the plaintiff from doing an act which he or she is lawfully entitled to do.[98]

74.64 His Honour noted that a defence of public interest should be available, but that no such defence had been made out on the facts of the case.[99]

74.65 In *Doe v Australian Broadcasting Corporation* (*Doe v ABC*), the defendant broadcaster published in its afternoon and evening radio news bulletins information that identified the plaintiff—a victim of a sexual assault.[100] In doing so, the defendant breached s 4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic), which makes it an offence in certain circumstances to publish information identifying the victim of a sexual offence. Hampel J in the County Court of Victoria held that, in addition to breaching a statutory duty owed to the plaintiff by virtue of the *Judicial Proceedings*

---

95 G Taylor and D Wright, 'Australian Broadcasting Corporation v Lenah Game Meats: Privacy, Injunctions and Possums: An Analysis of the Court's Decision' (2002) 26 *Melbourne University Law Review* 707, 709.

96 *Grosse v Purvis* (2003) Aust Torts Reports 81–706.

97 Ibid, [442].

98 Ibid, [444].

99 Ibid, [34].

100 *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

Reports Act, the defendant broadcaster and two of its employees were liable to the plaintiff in equity for breach of confidence, and in tort for invasion of privacy.[101]

74.66 In holding that a tort for invasion of privacy had been proved, Hampel J noted that

> this is an appropriate case to respond, although cautiously, to the invitation held out by the High Court in *Lenah Game Meats* and to hold that the invasion, or breach of privacy alleged here is an actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort.[102]

74.67 Responding to the repeated suggestion by defence counsel that recognition of a tort of invasion of privacy would be a 'bold step',[103] her Honour stated:

> If the mere fact that a court has not yet applied the developing jurisprudence to the facts of a particular case operates as a bar to its recognition, the capacity of the common law to develop new causes of action, or to adapt existing ones to contemporary values or circumstances is stultified. *Lenah Game Meats*, and the UK cases … in particular those decided since *Lenah Game Meats*, demonstrate a rapidly growing trend towards recognition of privacy as a right in itself deserving of protection.[104]

74.68 The decision in *Doe v ABC* was appealed, but the matter was settled on 4 March 2008. To date, no other Australian court has followed suit in recognising a cause of action for breach of privacy. In fact, the scant judicial commentary on the issue leans in the opposite direction.[105] In *Giller v Procopets*, Gillard J of the Supreme Court of Victoria noted that:

> Although it has been advocated from time to time that there should be a cause of action based on failure to respect the privacy of a person, both English and Australian law have not recognised a cause of action based upon breach of privacy.[106]

74.69 His Honour concluded that, 'in my opinion the law has not developed to the point where the law in Australia recognises an action for breach of privacy'.[107] The decision is *Giller* is now the subject of an appeal.

---

101 In *Giller v Procopets* [2004] VSC 113, an earlier case from the Victorian Supreme Court, Gillard J concluded that 'the law has not developed to the point where the law in Australia recognises an action for breach of privacy': *Giller v Procopets* [2004] VSC 113, [188]. See also *Kalaba v Commonwealth* [2004] FCA 763; leave to appeal refused: *Kalaba v Commonwealth* [2004] FCAFC 326. For a critique of *Giller*, see D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 361–363.

102 *Doe v Australian Broadcasting Corporation* [2007] VCC 281, [157].

103 Ibid, [157].

104 Ibid, [161].

105 See, eg, *Giller v Procopets* [2004] VSC 113; *Kalaba v Commonwealth* [2004] FCA 763; leave to appeal refused: *Kalaba v Commonwealth* [2004] FCAFC 326.

106 *Giller v Procopets* [2004] VSC 113, [187]. See also *Kalaba v Commonwealth* [2004] FCA 763; leave to appeal refused: *Kalaba v Commonwealth* [2004] FCAFC 326.

107 *Giller v Procopets* [2004] VSC 113, [188]. For a critique of this judgment, see D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 361–363.

NSWLRC Consultation Paper on invasion of privacy

74.70 As noted above, the NSWLRC has released a consultation paper that discusses whether a statutory cause of action for invasion of privacy should be introduced in that state. The NSWLRC reached the preliminary view that persons should be protected in a broad range of contexts from unwanted intrusions into their private lives or affairs.[108] A statutory model to ensure such protection was put forward for consultation.[109]

74.71 After an extensive review of developments in Australia and overseas, the NSWLRC considered four possible statutory models:

> 1 One general, non-specific right to seek redress for invasion of personal privacy.
>
> 2 A general cause of action for invasion of privacy, supplemented by a non-exhaustive list of the circumstances that could give rise to the cause of action.
>
> 3 A general cause of action for invasion of privacy, together with other specific statutory causes of action, for example, in respect of unauthorised surveillance activity.
>
> 4 Several narrower and separate causes of action based on various distinct heads of privacy.[110]

74.72 The second option, which was the one favoured by the NSWLRC, was modelled on the existing law in the Canadian provinces of British Columbia, Saskatchewan, Manitoba, Newfoundland and Labrador.[111] This also was the model upon which the Irish Privacy Bill was based.[112] Unlike the Canadian and Irish models, which frame the cause of action in tort, the NSWLRC suggested that the cause of action should be expressed in terms of a right of action for invasion of privacy, rather than as a tort of violation of privacy.

74.73 The NSWLRC suggested the following wording for a statutory cause of action:

> A person would be liable under the Act for invading the privacy of another, if he or she:
>
> (a) interferes with that person's home or family life;
>
> (b) subjects that person to unauthorised surveillance;
>
> (c) interferes with, misuses or discloses that person's correspondence or private written, oral or electronic communication;
>
> (d) unlawfully attacks that person's honour and reputation;

---

108 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [1.20].
109 Ibid, proposal 1.
110 Ibid, [6.2].
111 *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act 1978* RSS c P–24 (Saskatchewan); *Privacy Act* CCSM s P125 (Manitoba); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador).
112 Privacy Bill 2006 (Ireland).

> (e) places that individual in a false light;
>
> (f) discloses irrelevant embarrassing facts relating to that person's private life;
>
> (g) uses that person's name, identity, likeness or voice without authority or consent.
>
> This list should be interpreted as illustrative and not exhaustive.[113]

74.74 Having suggested that a general cause of action for invasion of privacy could be provided for by statute, the NSWLRC went on to discuss the essential elements of the cause of action. The defences to such a cause of action are also discussed. On these issues, the NSWLRC called for submissions and refrained from making any proposals.[114]

74.75 In the final chapter, the NSWLRC explored a range of common law, equitable and statutory remedies that could be available to a person who has had his or her privacy unlawfully invaded. The NSWLRC proposed that:

> The statute should provide that where the court finds that there has been an invasion of the plaintiff's privacy, the Court may, in its discretion, grant any one or more of the following:
>
> - damages, including aggravated damages, but not exemplary damages;
> - an account of profits;
> - an injunction;
> - an order requiring the defendant to apologise to the plaintiff;
> - a correction order;
> - an order for the delivery up and destruction of material;
> - a declaration;
> - other remedies or orders that the Court thinks appropriate in the circumstances.[115]

74.76 The ALRC understands that the NSWLRC intends to have its final report completed in mid-2008, after further consultations.

Recognising an action for breach of privacy in Australia

74.77 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether a cause of action for breach of privacy should be recognised by the courts or the legislature in Australia.[116]

---

113 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [6.32].
114 Ibid, [7.60].
115 Ibid, proposal 2.
116 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 1–2.

74.78 There was general support for the recognition of a cause of action for breach of privacy in the submissions that addressed the question.[117] A significant minority, however, expressed serious reservations.[118] Comment on the question was more widespread in consultations, and the support for and against was similar to that evidenced in submissions.

74.79 The comments in the submission of the Centre for Law and Genetics are representative of the types of comments expressed by those who favoured the enactment of a statutory cause of action.

> It is most surprising that the Australian courts have yet to develop common law or equitable principles for breach of privacy in Australia. Australia is becoming increasingly out of step with other common law jurisdictions in this regard. It may well be that the courts would be amenable to such a development, should the right case come before them. In the absence of common law or equitable protection, there is good justification for the development of legislation to fill the void.[119]

74.80 In support of its view that a cause of action for breach of privacy should be recognised, AAMI noted:

> International law is moving this way, thus it would be logical to include this concept. Social expectations are also moving in this direction, especially with the advent of the internet and digital technology. Preferred method is statutory, as it's a lot easier for businesses to digest and apply.[120]

74.81 The arguments raised by stakeholders against the enactment of a cause of action fell into the following categories:

- the privacy of Australians is adequately protected under the current regulatory regime;[121]
- recognition of a cause of action for breach of privacy is best left to incremental development at common law through the courts;[122] and

---

117 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007; J Carland and J Pagan, *Submission PR 42,* 11 July 2006; M Lyons and B Le Plastrier, *Submission PR 41,* 11 July 2006.

118 Telstra, *Submission PR 185,* 9 February 2007; Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; SBS, *Submission PR 112,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

119 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

120 AAMI, *Submission PR 147,* 29 January 2007.

121 Telstra, *Submission PR 185,* 9 February 2007; AXA, *Submission PR 119,* 15 January 2007; SBS, *Submission PR 112,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

- a statutory cause of action for breach of privacy would tip the balance too heavily in favour of privacy rights for individuals at the expense of the free flow of information on matters of public concern,[123] and the benefits to society flowing from artists who create art in public places, for example photographers.[124]

74.82 Media organisations, in particular, were concerned that a statutory cause of action for breach of privacy would 'be just another weapon in the arsenal of those in society who would seek to deflect public scrutiny of their possible malfeasance or non-feasance'.[125] The Australian Press Council (APC) stated:

> In the development of any proposal towards a putative cause of action for breach of privacy, the Commission needs to place a stress on the public interest as an appropriate criterion to be used to determine the balance between privacy rights for individuals and the public's right to the free flow of information on matters of public concern.[126]

Discussion Paper proposal

74.83 In DP 72, the ALRC proposed the introduction of a statutory cause of action for serious invasion of privacy, similar to that put forward by the NSWLRC.[127] The ALRC proposed that liability would be established where there was a reasonable expectation of privacy and the act complained of was sufficiently serious to cause substantial offence to a person of ordinary sensibilities.[128] The ALRC also proposed a non-exhaustive list of activities that could constitute an invasion of privacy, including:

- interference with an individual's home or family life;
- where an individual has been subjected to unauthorised surveillance;
- where an individual's correspondence has been interfered with, misused or disclosed; or
- where sensitive facts relating to an individual's private life have been disclosed.[129]

74.84 The proposed cause of action was subject to a number of limitations, these being that only natural persons should be allowed to bring an action and that the action

---

122 Telstra, *Submission PR 185*, 9 February 2007.
123 SBS, *Submission PR 112*, 15 January 2007; Australian Press Council, *Submission PR 83*, 12 January 2007.
124 Arts Law Centre of Australia, *Submission PR 125*, 15 January 2007.
125 Australian Press Council, *Submission PR 48*, 8 August 2006.
126 Ibid.
127 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 5–1.
128 Ibid, Proposal 5–2.
129 Ibid, Proposal 5–3(a), (c).

should be restricted to intentional or reckless acts on the part of the defendant.[130] Finally, the ALRC proposed that there should be no need to show proof of damage and that the cause of action should be subject to a number of exhaustive defences. These included that:

- the act or conduct was incidental to the exercise of a lawful right of defence of person or property;
- the act or conduct was authorised or required by or under law;
- disclosure of the information was of public interest or was fair comment on a matter of public interest; or
- disclosure of the information was privileged under defamation law.[131]

Submissions and consultations

74.85 There was strong support for the enactment of a statutory cause of action for a serious invasion of privacy.[132] The Office of the Privacy Commissioner (OPC) argued that such a development would

> clearly establish that privacy is an important human right that warrants specific recognition and protection within the Australian community, and in a way that accords with the community expectations and understanding of the meaning of 'privacy'. The Office reiterates its view that a dedicated privacy based cause of action could serve to complement the already existing legislative based protections afforded to individuals and address some gaps that exist both in the common law and legislation.[133]

74.86 The Public Interest Advocacy Centre (PIAC) argued that 'it is unacceptable that people who suffer flagrant invasions of their territorial or bodily privacy or the privacy of their communications have virtually no recourse under existing privacy laws'.[134]

74.87 Privacy NSW also broadly supported the inclusion of a statutory cause of action, but suggested that the matters could be dealt with in one of the model Unified Privacy Principles (UPPs).[135] Two stakeholders suggested that only those subject to the *Privacy*

---

130 Ibid, Proposals 5–1 to 5–7.
131 Ibid, Proposals 5–1 to 5–7.
132 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540,* 21 December 2007; Australian Lawyers Alliance, *Submission PR 528,* 21 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500,* 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.
133 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.
134 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.
135 Privacy NSW, *Submission PR 468,* 14 December 2007.

Act should be subject to the cause of action.[136] This would mean that agencies and organisations that were exempt from the operation of the *Privacy Act* would be immune from civil liability under the cause of action.

74.88 Some stakeholders opposing the introduction of a cause of action asserted that adequate restrictions are already in place and the cause of action would impose further restrictions on those already subject to rules under the *Privacy Act*.[137] The Law Council of Australia expressed the view that the existing federal co-regulatory scheme 'consisting of the *Privacy Act* and relevant media industry codes of practice provides appropriate and adequate recourse to individuals who consider that a media organisation has interfered with their privacy'.[138]

74.89 The Australian Bankers' Association submitted that it was unclear how the cause of action would co-exist with the model UPPs:[139]

> A cause of action will open up the prospect of class actions and opportunities for litigation funders resulting in encouragement to litigate because the plaintiff is generally protected from an adverse costs order if the action fails.[140]

74.90 The New South Wales Department of Corrective Services had no objection to the cause of action, as long as corrective services officers were able to carry out the functions, powers and duties conferred on them by Parliament. It suggested the addition of a defence that excludes law enforcement agencies from liability while carrying out their functions.[141]

74.91 One of the key concerns raised in submissions was that placing privacy protection on a statutory footing would interfere with other rights and interests, especially the right to freedom of expression and freedom of the press.

74.92 It is important to keep in mind, however, that 'freedom of expression' and 'freedom of the press' are not synonymous—although the latter often facilitates the former. Professor Eric Barendt has written that:

> Press freedom is parasitic to some extent on the underlying free speech rights and interests of readers and listeners, and the role which the press and other media play in informing them. It is not the same as the free speech argument, and that should be borne in mind when we consider how much weight should be attached to the freedom

---

136 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466*, 13 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007.

137 Australian Library and Information Association, *Submission PR 446*, 10 December 2007; ASTRA, *Submission PR 426*, 7 December 2007; Australian Information Industry Association, *Submission PR 410*, 7 December 2007; R Lake, *Submission PR 305*, 19 July 2007.

138 Law Council of Australia, *Submission PR 527*, 21 December 2007.

139 See Part D.

140 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

141 New South Wales Department of Corrective Services, *Submission PR 561*, 23 January 2008.

> when it conflicts with the right to privacy which certainly is a fundamental human right.[142]

74.93 While Barendt's comments are couched in the language of 'free speech rights', which are expressly recognised in the *United States Constitution*, the underlying rationale applies equally in an Australian context. The result is that publication of personal information may constitute an invasion of privacy if the privacy interest asserted by the claimant outweighs the public interest in freedom of expression asserted by the defendant.

74.94 As discussed in Chapter 42, freedom of expression is not an absolute right. The law limits many forms of expression, including speech that is obscene, defamatory or vilifies certain groups of people.

74.95 The ALRC received a number of submissions from professional and amateur street artists who were concerned that the cause of action would prohibit street art and the taking of photographs in public places.[143] The following is an example of the type of concern that was raised:

> The way I achieve my art is by strolling through streets and cities, photographing people and situations that depict a narrative of life and the world we live in. I'd like to think that the work I do is neither invasive nor arrogant ... but showing sides of life that happen every second of the day that many of us have become simply too busy to notice a lot of the time.
>
> My ability to do this relies on the fact that as it stands, I can practically photograph anything that is in 'public view'…[144]

74.96 Media organisations also reiterated the concerns expressed in response to IP 31. The Herald and Weekly Times Pty Ltd (HWT) submitted that it is critical that journalists are able to watch, film, record and gather information without any further restrictions:

> Clearly, the proposed laws will discourage journalists' sources who use surveillance techniques to collect information in pursuit of uncovering or confirming a story of public concern. This will result in curtailing of the free flow of information and

---

142 E Barendt, 'Privacy and Freedom of Speech' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 11, 23.

143 Australian Library and Information Association, *Submission PR 446*, 10 December 2007; Australian Network for Art and Technology, *Submission PR 434*, 10 December 2007; National Association for the Visual Arts Ltd, *Submission PR 415*, 7 December 2007; P Hammer, *Submission PR 396*, 7 December 2007; N Griffiths, *Submission PR 395*, 7 December 2007; Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007; R Anderson, *Submission PR 373*, 4 December 2007; E Halvorson, *Submission PR 367*, 3 December 2007; M Schaefer, *Submission PR 364*, 3 December 2007; O Esmonde-Morgan, *Submission PR 361*, 3 December 2007; H Page, *Submission PR 360*, 2 December 2007; K Purcell, *Submission PR 359*, 2 December 2007; J Mortelliti, *Submission PR 357*, 2 December 2007.

144 H Shaud, *Submission PR 366*, 4 December 2007.

> reducing the amount of stories the media will be able to uncover and reveal to the public.[145]

74.97 The HWT also argued that

> Similar to the balancing act required in establishing legislation for information privacy (resulting in the media exemption), questions regarding recognising an actionable right to personal privacy also requires consideration of the balance between the public interest in allowing the free flow of information to the public through the media and the public interest in adequately protecting an individual's right to privacy.[146]

74.98 The HWT submission offered a number of examples of stories that, in its view, would be in danger of remaining untold if the cause of action was enacted. Examples of current practices of journalists that could potentially constitute a serious invasion of privacy included:

- journalists knocking on the door of a person's home unannounced to collect information for a story. For example, journalists will often contact relatives of victims of road accidents;

- investigative journalists conducting surveillance or interviews in researching a story; and

- 'vox pops'—approaching someone in the street to ask him or her a question for the purpose of using his or her answer as an indicator of public opinion. Some types of questions asked may be considered to relate to 'private matters'.[147]

74.99 The APC did not support the introduction of a statutory cause of action for invasion of privacy. It noted that those countries in which a cause of action is available generally have either a constitutional or statutory protection for freedom of expression. The APC noted that it would not be appropriate to give effect to art 17 of the ICCPR without, at the same time, giving effect to art 19. It urged the ALRC to consider introducing the statutory protection of free speech as an 'essential concomitant' of any mechanism intended to increase the protection of personal privacy.[148]

---

145 The Herald and Weekly Times Pty Ltd, *Submission PR 568*, 11 February 2008.
146 Ibid.
147 Ibid.
148 Australian Press Council, *Submission PR 411*, 7 December 2007.

74.100 Concerns also were raised in submissions that the cause of action would chill marketing campaigns and, in particular, telemarketing and door-to-door sales.[149] The ANZ submitted that in pursuing the recovery of debts and the enforcement of security rights, 'it is difficult to avoid some direct interaction with home and family'.[150]

74.101 Some questioned whether there could be a reasonable expectation of privacy when an individual is in a public place. For example, one stakeholder stated:

> Privacy belongs in the home, in private. Once I step outside of my own home, others can see me for who I am and what I do. If I choose not to be seen, I will stay indoors.[151]

74.102 Stakeholders were divided about whether the 'use of another's name, identity, likeness or voice' should constitute an invasion of privacy. The APC was of the view that the notions of 'false light', damage to reputation and appropriation of likeness, which form part of the American *Restatement* formulation discussed above, should specifically be excluded from the scope of the cause of action.[152] However, a different view was put forward by the Media, Entertainment and Arts Alliance[153] and the AFL Players' Association. They suggested that the cause of action should include protection for name, identity, likeness and voice. The AFL used the following example:

> Anyone may distribute a collection of trading cards, videos, post cards, or calendars titled 'Unauthorised Schoolie Week Beach Shots' filled with candid photos of unsuspecting high school graduates in their bathing outfits. In that case it is not the schoolies' interest in commercialising their personalities that begs protection, but their privacy and personal dignity …
>
> Personality rights should not be denied privacy protection merely because a small segment of the community can derive a commercial benefit from such protection. No one should be permitted to intrude into an Australian's personal sphere.[154]

74.103 The Cyberspace Law and Policy Centre questioned whether 'offence' was the best way to describe the reaction required to trigger the cause of action, suggesting that 'offence or distress' would be more appropriate. The Centre submitted that this also would capture the situation where a defendant acted negligently (and therefore the claimant was not offended, but distressed).[155]

---

149 Australian Information Industry Association, *Submission PR 410*, 7 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

150 ANZ, *Submission PR 467*, 13 December 2007.

151 N Griffiths, *Submission PR 395*, 7 December 2007.

152 Australian Press Council, *Submission PR 411*, 7 December 2007.

153 Media Entertainment and Arts Alliance, *Submission PR 406*, 7 December 2007.

154 AFL Players' Association, *Submission PR 393*, 7 December 2007.

155 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

74.104 The APC and another stakeholder suggested that proof of damage should be an element of the cause of action.[156] While not supporting the cause of action, in principle, the APC stated:

> it would not be appropriate to allow a plaintiff to bring an action seeking compensation where that plaintiff is unable to adduce evidence of having suffered either injury or economic loss. If the aim of the action is to prevent publication in anticipation of a possible breach of privacy it would be more appropriate to encourage negotiation or mediation between parties. To facilitate the bringing of actions by plaintiffs who cannot demonstrate damage would be to encourage speculative actions in instances where only trivial breaches have occurred.[157]

Remedies

74.105 The APC disagreed with a number of the remedies proposed by the ALRC. In particular, it argued that the proposal to empower courts to order an account of profits as a remedy for breach of personal privacy was unworkable.

> Where the defendant in a privacy action is a publisher or other media organisation, it would be impossible to estimate the quantum of profits that might be derived from the alleged privacy intrusion.[158]

74.106 The APC also argued that injunctions could be exploited as a tool with which to obstruct freedom of expression:

> injunctions to prevent or delay publication impact not only upon the media but also affect groups of concerned citizens who seek to expose issues that have the potential to significantly affect the community. Such injunctions risk distorting or obstructing democratic processes and preventing scrutiny and accountability of developers, influential business people and public office holders.[159]

74.107 Concerns were raised about the inclusion of corrections and apologies in the remedies. In the APC's view, the possibility of a court-ordered correction or apology would act as a disincentive for out of court settlement. Defendants, the APC argued, would lose the capacity to offer something that the courts could not offer. It suggested that giving the courts power to grant other remedies or orders that the court thinks appropriate would create uncertainty and discourage attempts at settlement.[160]

74.108 In relation to apologies by the media, one individual commented that:

> Where it has been proven that claims were incorrect, particularly where they were made in the press, mandatory orders should be issued requiring the guilty party to not

---

156 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Australian Press Council, *Submission PR 411*, 7 December 2007. The Cyberspace Law and Policy Centre supported the ALRC's proposal: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

157 Australian Press Council, *Submission PR 411*, 7 December 2007.

158 Ibid.

159 Ibid. This view was shared by the Arts Law Centre: Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.

160 Australian Press Council, *Submission PR 411*, 7 December 2007. This view was shared by the Arts Law Centre: Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.

> only print a retraction or apology, but that it should be placed in the same place, in the same type face and on the same page as the original story. I often note how an apology in a newspaper is placed on a back page in small print in such a way that it is barely noticeable. If it was significant enough to command splashing across the front page or in the first few pages of a major tabloid, then any apology should receive the same importance.[161]

Defences

74.109 The Arts Law Centre of Australia submitted that there should be an exemption or defence for:

> - works and subject matter other than works (as defined in the *Copyright Act*) made for an artistic purpose or in the public interest; and
> - fair dealing uses similar to those in the *Copyright Act*, such as criticism and review, parody or satire, reporting the news, and research and study.[162]

74.110 The APC also recommended that the following should be included as defences to the cause of action:

- express or implied consent;
- the information is already in the public domain;
- where a person's privacy only is breached incidentally (for example, where the person photographed was in the background of a photo taken at a beach);
- the disclosure or publication was made for the purpose of rebutting an untruth made by the claimant; and
- where a journalist or publisher has given a fair report of court proceedings.[163]

Children

74.111 Youthlaw supported the introduction of a statutory cause of action for a serious invasion of privacy, but raised concerns about the legal capacity of children and young people to pursue privacy claims. Currently, children and young people need a litigation guardian appointed to bring a privacy claim. Youthlaw recommended that, where a young person is deemed to have capacity, he or she should be able to instruct a lawyer without the need for a litigation guardian.[164]

---

161 P Youngman, *Submission PR 394*, 7 December 2007.
162 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.
163 Australian Press Council, *Submission PR 411*, 7 December 2007.
164 Youthlaw, *Submission PR 390*, 6 December 2007.

ALRC's view

74.112 In the absence of a statutory cause of action for serious invasion of privacy, the common law in this area will continue to develop through the Australian courts. Whether this evolution results in the recognition of a tort of invasion of privacy, the adoption of the UK's approach to breach of confidence, a combination of the two, or a rejection of the international trend, is an open question.

74.113 If Australian courts follow the UK's approach of developing the cause of action within the equitable action for breach of confidence, or decide tort law should be the preferred vehicle, they will have to develop the cause or causes of action within the rules of equity and tort. This has an impact on the circumstances that will be recognised as giving rise to the cause of action, and on the remedies available to address the wrong.

74.114 Sir Roger Toulson, co-author of a leading text on confidentiality[165] and a judge of the England and Wales Court of Appeal, has highlighted, in the context of the UK's approach, a limitation inherent in the incremental development of the common law. He identifies an important limitation on the use of breach of confidence to address privacy issues.

> A consequence of the development of privacy within the action for breach of confidentiality is that it is presently confined to cases involving the use of information of a private nature, whether in word or pictorial form. So however strong and understandable may be the feeling of harassment of a person who is hounded by photographers when carrying out activities of a private nature, and however unacceptable the behaviour of the pack, there will be no cause of action until an intrusive photograph is published. From the viewpoint of the mischief against which Article 8 [of the *Human Rights Act 1998*] is aimed, this is illogical.[166]

74.115 To put these comments in an Australian context, if the UK's approach applied, the plaintiff in *Doe v ABC* would (and did on the findings of the trial judge) have a recognised cause of action for breach of confidence, but the claimant in *Grosse v Purvis* would be without a remedy.

74.116 Such constraints can be overcome if a statutory cause of action for serious invasion of privacy is enacted. This avoids the problems inherent in attempting to fit all the circumstances that may give rise to an invasion of privacy into a pre-existing cause of action—such as breach of confidence—or formulating a previously unrecognised cause of action—such as the tort of invasion of privacy. Enacting a statutory cause of action also allows for a more flexible approach to defences and remedies.[167]

---

165 R Toulson and C Phipps, *Confidentiality* (2nd ed, 2006).

166 R Toulson, 'Freedom of Expression and Privacy' (Paper presented at Association of Law Teachers Lord Upjohn Lecture, London, 9 February 2007), 7.

167 A case note on *Doe v ABC* published in the *Australian Press Council News* noted, 'if a privacy tort were defined by statute, it could incorporate workable defences. In addition to a strong public interest defence,

74.117 Individuals should be protected from unwanted intrusions into their private lives or affairs in a broad range of contexts, and it is the ALRC's view that a statutory cause of action is the best way to ensure such protection. It forecloses the possibility of Australian courts adopting an action in breach of confidence as the primary vehicle to protect an individual's private life from invasion, and alleviates the necessity of judges taking the 'bold step'[168] of formulating a new tort and a lengthy period of uncertainty and inconsistency as the courts refine the law in this area. Further, it does away with the distinction between equitable and tortious causes of action, and between the defences and remedies available under each.

74.118 The ALRC supports the view expressed in NSWLRC CP1 that the 'statutory cause of action for invasion of privacy should not be constrained at the outset by an assumption that rules otherwise applicable to torts generally should necessarily apply to the statutory cause of action for invasion of privacy'.[169] In addition, as the NSWLRC notes, this approach allows for the consideration of competing interests, including the public interest, 'that have not traditionally been relevant in the development of tortious causes of action'.[170]

74.119 In the ALRC's view, it is also appropriate to set out a non-exhaustive list of the types of acts or conduct that could constitute an invasion of privacy. This will be useful in indicating to the courts the scope of the action. Examples where an invasion of privacy may occur should include where:

- there has been a serious interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; and
- sensitive facts relating to an individual's private life have been disclosed.

74.120 In the ALRC's view, the cause of action should not include use of a person's identity or likeness without consent. It is questionable whether an unlawful attack on a person's honour and reputation, placing a person in a false light and using a person's name, identity, likeness or voice without authority or consent are properly characterised as invasions of privacy. It has been argued, at least in relation to false

---

a defence could be based on an appropriate offer-of-amends procedure': I Ryan, 'Doe v ABC—A Case Note' (2007) 19(2) *Australian Press Council News* <www.presscouncil.org.au>, 7.

168 *Doe v Australian Broadcasting Corporation* [2007] VCC 281, [157].

169 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [1.7].

170 Ibid, [1.7].

light and appropriation, that such conduct is better left to the law of defamation.[171] The same argument applies to an unlawful attack on a person's honour and reputation, which clearly falls within the parameters of defamation law.[172]

74.121 In *Lenah Game Meats*, Gummow and Hayne JJ commented on the tenuous nexus between privacy and the appropriation and false light torts.

> Whilst objection possibly may be taken on non-commercial grounds to the appropriation of the plaintiff's name or likeness, the plaintiff's complaint is likely to be that the defendant has taken the steps complained of for a commercial gain, thereby depriving the plaintiff of the opportunity of commercial exploitation of that name or likeness for the benefit of the plaintiff. To place the plaintiff in a false light may be objectionable because it lowers the reputation of the plaintiff or causes financial loss or both. The remaining categories [of the *Restatement of the Law, 2nd, Torts, 1977* (US)], the disclosure of private facts and unreasonable intrusion upon seclusion, perhaps come closest to reflecting a concern for privacy 'as a legal principle drawn from the fundamental value of personal autonomy', the words of Sedley LJ in *Douglas v Hello! Ltd*.[173]

74.122 It has also been suggested that the appropriation tort is a form of intellectual property, in that it protects a property right as distinct from the privacy of a person. Alternatively, an extension of the tort of 'passing off', or the development of a 'right of publicity', may be a better way to deal with the perceived problem.[174]

74.123 It is undesirable for the cause of action to be used as an intellectual property style personality right to protect commercial value. This type of scenario may be illustrated by reference to *Douglas v Hello!*[175] where the plaintiffs claimed the privacy of their wedding photographs in order to protect the commercial value of the photographs that they had sold to a rival magazine. Consequently, it is undesirable expressly to include 'use of another's name, identity, likeness or voice' in the list of types of intrusion that will ground the cause of action for serious invasion of privacy.

74.124 Circumstances giving rise to the cause of action should not be limited to activities taking place in the home or in private places. Clear lines demarcating areas in which privacy can be enjoyed should not be drawn in advance, since each claim will have to be judged in its particular context. The appropriate test is whether the

---

171 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 368.

172 See, eg, s 3(c) of the uniform *Defamation Act 2005* in force in New South Wales, Victoria, Queensland, Western Australia, South Australia, Tasmania, and the Northern Territory.

173 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [125].

174 For a discussion of the application to appropriation cases of intellectual property law, the tort of 'passing off' and the development of a 'right of publicity', see R Zapparoni, 'Propertising Identity: Understanding the United States Right of Publicity and its Implications—Some Lessons for Australia' (2004) 28 *Melbourne University Law Review* 690. For a discussion of information privacy as a form of property, see J Rule, 'Towards Strong Privacy: Values, Markets, Mechanisms, and Institutions' (2004) 54 *University of Toronto Law Journal* 183. A contrary view is discussed in R Toulson and C Phipps, *Confidentiality* (2nd ed, 2006), [2–056]–[2–066].

175 *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920.

circumstances give rise to a reasonable expectation of privacy, regardless of whether the activity is in public or private.

74.125 In *Lenah Game Meats*, Gleeson CJ noted that 'an activity is not private just because it is not done in public'.[176] In the alternative, the fact that an activity takes place in public does not mean that an expectation of privacy cannot arise. In *Hosking v Runting*, a reasonable expectation of privacy did not arise because the photographs were taken in public *and* disclosed 'nothing more than could have been observed by an member of the public in Newmarket on that particular day'.[177] In *Campbell*,[178] the activity photographed was in public, but it revealed information about Campbell's health, a category of information that has long been considered sensitive and private.

74.126 One commentator has suggested that a reasonable expectation of privacy may arise in public where a person is

> involuntarily experiencing an intimate or traumatic experience in public, they are in a place where they reasonably perceive themselves to be reasonably imperceptible, or the defendant has used technological devices to penetrate his or her clothes or other self protection barriers.[179]

74.127 While leaving it open to the courts to determine when a reasonable expectation of privacy exists, the ALRC supports the narrower view of when a public act can be private, as expressed in *Campbell* rather than the more expansive view of the European courts in cases like *Von Hannover*, discussed above.[180]

74.128 The ALRC notes the concerns raised by Youthlaw, and considers a number of issues related to capacity, young people and privacy in Chapters 68 and 69. The issue of the capacity of young people generally to bring claims without a litigation guardian, however, is outside the Terms of Reference for this Inquiry.

Elements of a statutory cause of action

74.129 The NSWLRC suggested two possible approaches to establishing the elements of a statutory cause of action for invasion of privacy.

> An invasion of privacy could be determined as made out where:
>
> - The plaintiff had, in all the circumstances, a reasonable expectation of privacy in relation to the relevant conduct or information; and/or

176 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].
177 *Hosking v Runting* [2005] 1 NZLR 1, [164].
178 *Campbell v MGN Ltd* [2004] 2 AC 457.
179 M Moreham, 'Privacy in Public Places' (2006) 65 *Criminal Law Journal* 606.
180 In the ALRC's view, the interpretation of *Von Hannover*, suggested by Professor Phillipson, is the preferable approach for Australian courts to adopt.

- The defendant's invasion of that privacy in relation to that conduct or information, is, in all the circumstances, offensive (or highly offensive) to a reasonable person of ordinary sensibilities.[181]

74.130 The fact that the two approaches are not mutually exclusive is evidenced by the decision in *Hosking v Runting*.[182] As noted above, the court found that the fundamental requirements for a successful interference with privacy, in the context of wrongful publicity given to private lives, includes both (a) a reasonable expectation of privacy; and (b) conduct that would be considered highly offensive to the hypothetical reasonable person.

74.131 The NSWLRC concedes that these two approaches 'may often be two sides of the same coin. They are not necessarily mutually exclusive'. However, this may not always be the case. To illustrate the point, the NSWLRC gives the example of a medical practitioner who reveals the claimant's HIV status by mistake. The NSWLRC suggests that the claimant may have a reasonable expectation of privacy, but that the disclosure of the claimant's HIV status will not be 'highly offensive to a reasonable person of ordinary sensibilities'.[183]

74.132 Such a distinction illustrates the point made by Nicholls LJ in *Campbell*, noted above. The 'highly offensive' formulation should be approached with care, one reason being that the phrase 'highly offensive' is suggestive of a stricter test of what should be considered private than 'a reasonable expectation of privacy'.[184]

74.133 In determining what is considered 'private' for the purpose of establishing liability under the statutory cause of action, the ALRC's preference is that there should be *both* a reasonable expectation of privacy in all the circumstances, and the act complained of must satisfy an objective test of seriousness.

74.134 In DP 72, the ALRC expressed concern that adopting the phrase 'highly offensive to a reasonable person of ordinary sensibilities', used by Gleeson CJ in *Lenah Game Meats*,[185] may be too high a threshold, and suggested that the test should be whether the act in question was 'sufficiently serious to cause substantial offence'.[186]

74.135 After further consultation and reflection, however, the ALRC now accepts that the higher bar is preferable for the statutory cause of action. Setting a high threshold to establish a serious invasion of privacy is consciously intended to ensure that freedom of expression is respected and not unduly curtailed in the great run of circumstances—the cause of action only will succeed where the defendant's conduct is thoroughly

---

181 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.5].
182 *Hosking v Runting* [2005] 1 NZLR 1, [117].
183 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.6].
184 *Campbell v MGN Ltd* [2004] 2 AC 457, [22].
185 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].
186 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [5.80].

inappropriate and the complainant suffered serious harm as a result. This formula also offers a number of other advantages, including simplifying the law and providing courts with some guidance on its application—particularly given that the statutory test will be consistent with developments in the common law in Australia and New Zealand.

74.136 The characterisation of the cause of action as a 'serious invasion of privacy' also will clarify the types of matters intended to be covered by the action, and allay many of the concerns raised in submissions. For example, street art generally would not fall within the scope of the cause of action. A claimant simply captured in a photograph of a street scene, taken in the manner suggested in some of the submissions, is unlikely to be able to establish either that there was a reasonable expectation of privacy or that the act complained of would be highly offensive to a reasonable person of ordinary sensibilities.

74.137 It is neither feasible nor desirable to attempt to list or limit the types of acts that may be found to be highly offensive to a reasonable person of ordinary sensibilities. As noted above, matters the ALRC previously considered to be worthy of protection through a cause of action include sensitive facts relating to a person's individual relationships, health, home, family and private life.[187] Acts or disclosures revealing this type of sensitive or intimate information are the most likely to meet the test of what would be highly offensive.

74.138 Protecting such information should not hinder legitimate investigative journalism as described by media groups to this Inquiry. For example, allegations of misconduct or corruption in public life would not fall within this zone of protection.

74.139 To illustrate this point more clearly, the ALRC provides below some examples of the circumstances that the ALRC considers should amount to a serious invasion of privacy for the purposes of the recommended cause of action.

187 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [236].

Examples of matters intended to fall within the ALRC's recommended statutory cause of action for serious invasion of privacy

1. Following the break-up of their relationship, Mr A sends copies of a DVD of himself and his former girlfriend (B) engaged in sexual activity to Ms B's parents, friends, neighbours and employer.[188]

2. C sets up a tiny hidden camera in the women's toilet at his workplace, capturing images of his colleagues that he downloads to his own computer and transmits to a website hosted overseas, which features similar images.[189]

3. D works in a hospital and accesses the medical records of a famous sportsman, who is being treated for drug addiction. D makes a copy of the file and sells it to a newspaper, which publishes the information in a front page story.[190]

4. E runs a small business and uses F&Co Financial Advisers to handle her tax affairs and financial advice. Staff at F&Co decide to do a bit of 'spring cleaning', and a number of files are put out in a recycling bin on the footpath—including E's file, which contains her personal and contact details, tax file and ABN numbers, and credit card details. A passerby grabs the file and, unbeknown to E, begins to engage in identity theft: removing money from E's bank account, using her credit cards and applying for additional credit cards in E's name.[191]

188 This example is loosely drawn from the circumstances in *Giller v Procopets* [2004] VSC 113 and *Grosse v Purvis* (2003) Aust Torts Reports 81–706.

189 This example is loosely drawn from the circumstances described in D Emerson, 'SBS: Camera in Change Room', *Sydney Morning Herald*, 5 May 2008, <www.smh.com.au>; L McKenny, 'SBS Ignored Peeping Tom Alert: Inquiry', *Sydney Morning Herald*, 22 May 2008, <www.smh.com.au>; and 'Perve Films Flatmate with Teddy Bear Camera', *Sydney Morning Herald*, 24 April 2008, <www.smh.com.au>.

190 This example is loosely drawn from the circumstances in 'AFL Up in Arms Over Records Leak', *ABC News Online*, 29 April 2007, <www.abc.net.au>; C Ornstein, 'UCLA Workers Snooped in Spears' Medical Records', *Los Angeles Times*, 15 March 2008, <www.latimes.com>; and R Goldman, 'Clooney Proves Private Health Records Not So Private', *ABC News (US)*, 11 October 2007, <www.abcnews.go.com>.

191 This example is loosely drawn a number of 'files on the footpath' cases, including M Moore, 'Private Files Put on Street for All to Read', *Sydney Morning Herald*, 6 May 2008, <www.smh.com.au>; A Falk, 'Health Files are Sold as Scrap Paper to Utah', *Deseret News*, 10 March 2008 <deseretnews.com>; 'Report Details Private Health Records Misplaced in Public Places', *ABC News Online*, 4 October 2006, <www.abc.net.au>.

74.140 While some of the examples above also may give rise to criminal sanctions,[192] a federal statutory cause of action would give complainants access to a broader range of civil remedies to redress the invasion of their privacy. In the case of *Giller v Procopets*,[193] the defendant showed another person a video of himself and the plaintiff having sex, left a copy of the video with the plaintiff's father and threatened to show the video to others, including the plaintiff's employer—and it was found that, under the existing state of the law, the plaintiff was left with no remedy in either criminal or civil law.

74.141 A number of stakeholders in this Inquiry have claimed that there have not been a sufficient number of complaints to warrant enactment of a cause of action for a serious invasion of privacy. The ALRC suggests that there are two arguments against the logic of that claim. First, the fact that no cause of action currently exists (and the lack of a definitive judgment under the common law) means that the numbers of those who have experienced a serious invasion of privacy cannot be known. Secondly, effective law reform must respond not only to current problems and gaps in the law, but also anticipate where there are likely to be significant problems in the future that will require some kind of regulation. In this case, it is clear that developments in information technology and surveillance technology have led to widespread concerns about an 'increasingly invasive social environment'.[194]

74.142 In Chapter 11, the ALRC discusses the many submissions this Inquiry received about the permanence of personal information published on the internet by individuals.[195] As well as sites such as Facebook and YouTube, where individuals can post photographs or videos, there are at least 100 websites that contain images of people caught showering or undressing.[196] The ALRC notes the limitations of using 'take-down' notices where a person is posting information on the internet in a personal capacity. The utility of establishing an Australian take-down notice scheme is also questionable, given the ease of moving internet content to a website hosted in another

---

192 For example, the *Crimes Act 1900* (NSW) creates offences of peeping or prying or stalking. In addition, the *Summary Offences Act 1988* (NSW) creates an offence of filming someone without their consent for a sexual purpose.

193 *Giller v Procopets* [2004] VSC 113.

194 *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920, [111], cited in New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [123].

195 See, eg, Health Informatics Society of Australia, *Submission PR 554*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Australia's National Computer Emergency Response Team, *Submission PR 474*, 14 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007; J Watts, *Submission PR 302*, 10 July 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

196 C Calvert, *Voyeur Nation: Media, Privacy, and Peering in Modern Culture* (2000), cited in D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 100.

jurisdiction. In these cases, a more appropriate remedy would be available through a statutory cause of action for a serious invasion of privacy.

A balancing test

74.143 As noted above, a number of stakeholders argued that placing privacy protection on a statutory footing would give inappropriately great weight to privacy rights at the expense of other rights and interests. In DP 72, the ALRC proposed that the issues of freedom of expression and fair reporting by the press on a matter of public interest be dealt with in the defences to the cause of action, by including as a defence information disclosed as a matter of public interest or a fair comment on a matter of public interest.[197]

74.144 Some stakeholders suggested that the reference to freedom of expression and fair comment by the media in the defences may be problematic. Arguably, it would allow unmeritorious claims to proceed, with defendants being forced to wait until the defence case was called before evidence supporting the defence case was led.

74.145 The ALRC agrees with the APC that the public interest in allowing freedom of expression is an essential criterion to be used to determine 'the balance between privacy rights for individuals and the public's right to the free flow of information on matters of public concern'.[198]

74.146 As discussed in Chapter 5, the right to privacy is one of a number of fundamental human rights set out in the ICCPR and other international instruments. The right is not absolute, and privacy competes with other rights and interests, such as freedom of expression. In *McKennitt v Ash*, Eady J noted that the balancing of these rights does not occur in a vacuum and public attitudes towards the correct balancing of rights may change along with societal expectations:

> It is clear that [in the United Kingdom] there is a significant shift taking place as between, on the one hand, freedom of expression for the media and the corresponding interest of the public to receive information, and, on the other hand, the legitimate expectation of citizens to have their private lives protected … Even where there is a genuine public interest, alongside a commercial interest in the media in publishing articles or photographs, sometimes such interests would have to yield to the individual citizen's right to the effective protection of private life.[199]

74.147 Rather than attempt to protect other rights through a defence, the ALRC agrees it would be better in principle and in practice to add an additional element to the cause of action for a serious invasion of privacy. This would ensure that privacy interests are not privileged over other rights and interests.[200]

---

197 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 5–5.

198 Australian Press Council, *Submission PR 48*, 8 August 2006.

199 *McKennitt v Ash* [2005] EMLR 10, [57].

200 This was also the view taken by the ALRC in regards to the review of sedition offences in 2006. Those offences contained a defence for media, which the ALRC recommended should be changed to require the

74.148 One option would be to require the courts to balance the privacy claim against any other rights and important public interests when determining whether the cause of action is established. In particular, freedom of expression in its broader sense should be considered a key public interest. Other public interests that were identified by the NSWLRC as potentially likely to arise in the context of an invasion of privacy are: matters relating to national security; the commission of criminal conduct; and threats to public health and safety.[201]

74.149 Article 19 of the ICCPR states that:

> (1) Everyone shall have the right to hold opinions without interference.
>
> (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> (3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> a) For respect of the rights or reputation of others;
>
> b) For the protection of national security or of public order (ordre public), or of public health or morals.

74.150 Freedom of expression is given some limited forms of protection in Australian law—particularly under the *Australian Constitution*, which is discussed below. The common law, and some federal, state and territory legislation, also provide limited protection to certain categories of expression.[202] For instance, all Australian jurisdictions are subject to at least one 'freedom of information' regime, the objectives of which include the fostering of public debate and discussion.[203]

74.151 As noted in Chapter 42, notwithstanding the absence of explicit constitutional protection for free speech, in a series of cases culminating in *Lange v Australian Broadcasting Corporation*, the High Court has held that the *Australian Constitution* must be read as impliedly protecting a particular category of expression—namely,

---

trier of fact to take into account whether the conduct was done in specific circumstances: Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Rec 12–2.

201 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.37].

202 See M Chesterman, *Freedom of Speech in Australia: A Delicate Point* (2000), 7–13.

203 *Freedom of Information Act 1982* (Cth); *Freedom of Information Act 1989* (NSW); *Freedom of Information Act 1982* (Vic); *Freedom of Information Act 1992* (Qld); *Freedom of Information Act 1992* (WA); *Freedom of Information Act 1991* (SA); *Freedom of Information Act 1991* (Tas); *Freedom of Information Act 1989* (ACT); *Information Act 2002* (NT).

political communication.[204] Other jurisdictions, such as the UK[205] and New Zealand,[206] recognise freedom of expression in a statutory bill of rights.

74.152 Regardless of whether it is protected by a constitutional or a statutory bill of rights, freedom of expression tends to be conceived, and protected, in a manner that is broadly consistent with the approach taken in art 19 of the ICCPR.[207] In other words, freedom of expression is regarded as a human right of fundamental importance—though, in certain circumstances, even this right must be reconciled with other competing rights or interests.

74.153 The *Human Rights Act 1998* (UK) includes a provision in s 12 which requires the courts to have particular regard to freedom of expression and art 10 of the ECHR when granting any relief which may impact on freedom of expression.

74.154 Although Australia is a signatory to the ICCPR, it would be difficult for the test under this cause of action to require the balancing of 'privacy rights' with the 'right to freedom of expression', as neither right has been given effect in domestic legislation, except in relation to information privacy under the *Privacy Act.* The ALRC also recommends the adoption of a broader conception of freedom of expression than is currently contained in the High Court cases which have found the existence of an implied constitutional right.[208] In particular, protection should not be limited to political speech. Nor should it be limited only to reporting by the media, as artistic and other creative works could also fall within 'freedom of expression'.

74.155 Chapter 5 notes that, although the right to privacy is an individual right, there is a strong public interest in protecting that right. There is also a public interest in allowing freedom of expression, and the free flow of information, in an open and democratic society.[209] A statutory cause of action would provide an opportunity to ensure that the appropriate balance between the public interests in protection of privacy and freedom of expression (and other public interests) is struck. Recognition of these other public interests simply reflects the fact that the right to privacy is not absolute. In appropriate circumstances, it will have to give way to other competing interests.

74.156 As noted above, and in Chapter 5, public interests can be, and frequently are, balanced against each other by the courts. In the traditional breach of confidence cases under the common law, the court can determine that the public interest in the protection of confidences is outweighed by a greater public interest in disclosure.[210] In

---

204 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
205 *Human Rights Act 1998* (UK) ss 12–13.
206 *New Zealand Bill of Rights Act 1990* (NZ) ss 13–14.
207 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 10 December 1948, Council of Europe, ETS No 005, (entered into force generally on 3 September 1953).
208 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
209 *Hinch v Attorney-General (Vic)* (1987) 164 CLR 15, 86 (Gaudron J).
210 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.29], citing *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109.

the protection of confidential information under s 126 of the *Evidence Act 1995* (NSW), the court must balance a number of public interests, including the probative value of the evidence in the proceeding and the nature of the offence, with the likelihood of harm to the protected confider in adducing the evidence, and then decide if it is appropriate to give a direction under the section.

74.157 The ALRC, therefore, recommends that, in determining whether an individual's privacy has been invaded for the purpose of establishing the cause of action for serious invasion of privacy, the court must take into account whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest—including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression.

The role of consent

74.158 In most cases, consent—whether express or implied by the claimant or some person entitled to consent on the claimant's behalf—will provide an answer to a cause of action for invasion of privacy. Legislatively, it can be dealt with in the following ways.[211] It can:

- be included as an essential element of the cause of action—for example, to use 'letters, diaries or other personal documents of a person … *without the consent, express or implied, of the person or some other person who has the lawful authority to give the consent*', may in a variety of circumstances constitute an invasion of privacy;[212]

- be considered when determining whether there was a reasonable expectation of privacy in all the circumstances, or as a circumstance in determining whether the act complained of meets the test of 'sufficiently serious to cause substantial offence to a person of ordinary sensibilities';

- operate as an exception to the general cause of action;[213] or

- be a defence to an action.[214]

74.159 While one stakeholder argued that consent should be included as a defence to an action, in the ALRC's view, issues of consent are best dealt with in terms of an essential element of the cause of action. In particular, consent should be considered

---

211 Generally see Ibid, [7.12]–[7.17].

212 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 3(d) (emphasis added).

213 *Privacy Act 1996* RSBC c 373 (British Columbia) s (2)(a).

214 *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 5(1)(a); *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 4(1)(a); *Privacy Act* CCSM s P125 (Manitoba) s 5(a). See also, Hong Kong Law Reform Commission, *Civil Liability for Invasion of Privacy* (2004), recs 4, 9.

when determining whether the claimant had a reasonable expectation of privacy in the circumstances or when determining whether the act complained of was sufficiently serious to cause substantial offence to a person of ordinary sensibilities. This is consistent with the approach to consent adopted in the protection of personal information. Consent should be considered in the first instance when determining whether there has been a breach of the privacy principles, not as a defence to justify a breach.[215]

Natural persons

74.160 In DP 72, the ALRC proposed that the cause of action only be available for natural persons,[216] on the basis that the desire to protect privacy is founded on notions of individual autonomy, dignity and freedom.[217] In Chapter 7, the ALRC discusses the reasons why privacy laws are restricted to individuals, and supports the view that it is not appropriate to extend privacy protection to corporations and other commercial entities. Extending the protection of a human right to an entity that is not human is inconsistent with the fundamental approach of Australian privacy law.

Intentional or reckless acts

74.161 An act is intentional when the defendant deliberately or wilfully invades the plaintiff's privacy. Section 5.4 of the *Criminal Code* (Cth) defines 'recklessness' as follows:

> (1) A person is reckless with respect to a circumstance if:
>
> (a) he or she is aware of a substantial risk that the circumstance exists or will exist; and
>
> (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
>
> (2) A person is reckless with respect to a result if:
>
> (a) he or she is aware of a substantial risk that the result will occur; and
>
> (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
>
> (3) The question whether taking a risk is unjustifiable is one of fact.
>
> (4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

74.162 The Law Reform Commission of Hong Kong, in recommending a cause of action for intrusion into the solitude, seclusion or private affairs of another person, rejected the suggestion that a plaintiff should be allowed to recover for accidental or negligent intrusions. It was of the view, however, that liability should lie for reckless intrusions:

---

215 The role of consent in the context of the model UPPs is discussed in detail in Ch 19.

216 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 5–3.

217 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 225.

> Since indifference to the consequences of an invasion of privacy is as culpable as intentionally invading another's privacy, we consider that an intrusion must be either intentional or reckless before the intruder could be held liable.[218]

74.163 The NSWLRC suggested that 'including liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far'.[219]

74.164 The ALRC agrees with the NSWLRC, and recommends that the fault element of the cause of action for invasion of privacy should be restricted to intentional or reckless acts on the part of the respondent.

Proof of damage

74.165 The statutes of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador providing for the tort of violation of privacy all specify that the tort of violation of privacy is actionable without proof of damage. In other words, the cause of action is actionable *per se*—there is no requirement on the claimant to prove that any actual damage arose from the invasion of privacy.

74.166 In this regard, the Canadian tort of invasion of privacy differs from the tort of negligence, in that proof of damage is an essential element of the latter. The treatment of the tort of invasion of privacy is, therefore, more akin to trespass to the person or defamation, which are actionable without proof of damage.

74.167 Following this course would allow for an award of compensation for insult and humiliation.[220] It also would allow the court to award a wider range of remedies to address the invasion—for example, an order requiring the respondent to apologise to the claimant.

74.168 Finally, providing that invasion of privacy is actionable without proof of damage is itself recognition that the cause of action protects a fundamental human right, which should not be dependent on proof of damage flowing from the breach.[221]

Defences

74.169 The defences to a cause of action for invasion of privacy in other jurisdictions generally include:

- the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

---

218 Hong Kong Law Reform Commission, *Civil Liability for Invasion of Privacy* (2004), [6.71].
219 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.24].
220 F Trindade and P Cane, *The Law of Torts in Australia* (3rd ed, 1999), 23.
221 For a discussion of the status of privacy as a human right, see Ch 1.

- the act or conduct was authorised or required by or under law;
- the disclosure of information was of public interest or was fair comment on a matter of public interest; or
- the disclosure of information was, under defamation law, privileged.[222]

74.170 As noted above, the ALRC considers that the defence of disclosure in the public interest or fair comment on a matter of public interest should form part of the elements of the cause of action.

Required or authorised by or under law

74.171 Another important defence is that the act or conduct was required or authorised by or under law. This defence assumes particular importance in the context of law enforcement and national security.

74.172 In Chapter 16, the scope of this exception in the context of the *Privacy Act* is discussed in detail. The *Privacy Act* generally should not fetter a government's discretion to require or authorise that personal information be handled in a particular way. It follows, therefore, that a requirement that the act or conduct was required or authorised by or under law would be a defence to the statutory cause of action. As discussed in Chapter 16, the ALRC's view is that the definition of 'law' for the purposes of the 'required or authorised by or under law' exception should include Commonwealth and state and territory Acts and delegated legislation as well as duties of confidentiality under common law or equity.[223]

Other defences

74.173 The requirement for the court to balance the public interest in maintaining the claimant's privacy against other public interests, including freedom of expression, will address many of the concerns raised by the APC, and other media and arts interest groups.

74.174 Consequently, the additional defences of consent, information already being in the public domain, and disclosure for the purpose of rebutting an untruth—as proposed by the APC—are unnecessary. If the claimant had consented to the invasion of his or her privacy or the information was already public, it is unlikely that the elements of the cause of action would be satisfied. In other words, the claimant would not have a

---

222 See, eg, *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 5; Privacy Bill 2006 (Ireland) cl 5(1), 6. For the types of disclosure covered by privilege in defamation law, see ss 27 and 30 of the Uniform *Defamation Act 2005* in force in New South Wales, Victoria, Queensland, Western Australia, South Australia, Tasmania and the Northern Territory.

223 As such, the concerns raised by the New South Wales Department of Corrective Services would fall under this defence.

reasonable expectation of privacy nor would publication be highly offensive to a reasonable person of ordinary sensibilities.

74.175 Publication made for the purpose of rebutting an untruth on behalf of a claimant is already adequately covered by the public interest test. This is illustrated by *Campbell*[224] where the fact that Campbell was a drug addict was conceded by Campbell to be a publishable fact—there was a public interest in correcting the public statements made that she did not use drugs.

Remedies

74.176 In NSWLRC CP 1, the NSWLRC, as noted above, articulates the range of remedies that could be used to address an invasion of privacy. Given the wide range of circumstances in which an action for invasion of privacy may be brought under the statute, the ALRC agrees with the NSWLRC that it makes sense to 'enable the court to choose the remedy that is most appropriate in the fact situation before it, free from the jurisdictional constraints that may apply to that remedy in the general law'.[225]

74.177 In DP 72, the ALRC proposed that the following remedies should be available:

(a) damages, including aggravated damages, but not exemplary damages;

(b) an account of profits;

(c) an injunction;

(d) an order requiring the respondent to apologise to the claimant;

(e) a correction order;

(f) an order for the delivery up and destruction of material; and

(g) a declaration.[226]

74.178 In response to the concerns expressed by the APC that an account of profits could be unworkable, the ALRC notes that courts only would choose to apply this in circumstances where an account of profits could be determined. An account of profits is an equitable remedy for breach of confidence, breach of fiduciary duty and infringement of intellectual property.[227] It has been acknowledged, in those contexts,

---

224 *Campbell v MGN Ltd* [2004] 2 AC 457.
225 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [8.3].
226 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 5–6.
227 M Tilbury, *Civil Remedies* (1990), [4079].

that it may be hard to determine a defendant's 'profit', because of difficulties determining how much of the profit is attributable to the breach and how much to other factors (such as the defendant's skill). Nonetheless, courts have said that this difficulty will not preclude assessment, where possible.[228] An account of profits was included as one of the remedies in the Irish Privacy Bill.[229]

74.179 The ALRC does not agree that the availability of a court-ordered apology will lead to a disincentive on the part of claimants to settle. The main incentive for an out of court settlement is to save time, costs and the possible emotional trauma of a court hearing.

74.180 Therefore, the ALRC does not recommend any change to the proposal as set out in DP 72.

Should the statutory cause of action be in federal legislation?

74.181 Having recommended statutory recognition of a cause of action for a serious invasion of privacy, a question arises about where the cause of action should be located.

74.182 Inconsistency and fragmentation of laws regulating the handling of personal information were major issues in this Inquiry.[230] To avoid a similar problem arising in relation to the enactment of a statutory cause of action for invasion of privacy, it is desirable to ensure national consistency from the outset. Models for achieving national consistency are canvassed in detail in Chapter 3.

74.183 Supporters of a statutory cause of action also issued a plea for uniformity. The Centre for Law and Genetics, for example, stated that, if a statutory cause of action were developed, 'it is critically important that it should be consistent across Australia, either as uniform state and territory legislation through agreement between the relevant Ministers, or as federal legislation'.[231] The OPC noted that

> it would be preferable to introduce a tort of privacy in a uniform manner throughout Australia, particularly to avoid inconsistencies and 'forum shopping' … Nevertheless, by what method a tort would be established and in what manner it would be introduced, it should not contribute to the national inconsistency that currently exists in the privacy laws arena.[232]

74.184 Most of those in favour of a statutory cause of action expressed the view that it should be enacted in federal legislation. The Queensland Government, for example, recommended that, 'if implementation of a statutory cause of action for breach of

---

228 *Docker v Somes* (1834) 39 All ER 1094, 1101.

229 Privacy Bill 2006 (Ireland), cl 8. See also New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [8.30].

230 See Part C.

231 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

232 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

privacy is proposed, such a cause of action should be located in federal legislation'.[233] Similarly, AAMI stated, 'the legislation should definitely be federal (one set of rules for the whole country). The *Privacy Act* is the logical place for it'.[234]

74.185 Professor Graham Greenleaf, Nigel Waters and Associate Professor Lee Bygrave of the Cyberspace Law and Policy Centre suggested that:

> Given that the Commonwealth has asserted constitutional power in relation to the protection of privacy in the private sector, it may be consistent with this for the Commonwealth to also legislate, in the *Privacy Act*, for a statutory tort or torts to protect other aspects of privacy in relation to the private sector. It will be necessary to carefully align the elements of a statutory privacy tort with what is already protected by privacy principles.[235]

74.186 For the reasons outlined in Chapter 3, the ALRC considers that the federal government has the constitutional power to enact a statutory cause of action for serious invasion of privacy, to the exclusion of state and territory legislation. The federal government could decide, however, to include a provision that provides that the federal Act is not intended to exclude or limit the operation of a law of a state or territory that is capable of operating concurrently with the federal Act.[236] If the latter policy option prevails, it is essential to ensure that the states and territories enact uniform legislation. Failure to do so would give rise to the fragmentation and inconsistency that has characterised the regulation of information privacy to date.

74.187 The ACT Department of Justice and Community Safety expressed concern that a cause of action for serious invasion of privacy may be enacted to the exclusion of state and territory legislation. In particular, the Department expressed concern that the *Human Rights Act 2004* (ACT) should not be excluded or limited by the operation of the statutory cause of action. Consequently, it would support the inclusion of an express provision in any federal legislation to the effect that the statutory cause of action is not intended to exclude or limit the operation of state and territory laws such as the *Human Rights Act*.[237]

74.188 The South Australian Government did not support any move to apply the cause of action to state public sectors through application of the *Privacy Act* to state bodies.[238]

---

233 Queensland Government, *Submission PR 242*, 15 March 2007.
234 AAMI, *Submission PR 147*, 29 January 2007.
235 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.
236 For an example of such a provision, see the *Age Discrimination Act 2004* (Cth) s 12(3).
237 ACT Department of Justice and Community Safety, *Submission PR 577*, 12 March 2008.
238 Government of South Australia, *Submission PR 565*, 29 January 2008.

74.189 In the ALRC's view, to ensure uniformity and to avoid the problems associated with inconsistent legislation, the statutory cause of action for invasion of privacy should be in federal legislation and should cover federal agencies, organisations and individuals. It also should cover state and territory public sector agencies, subject to any of the constitutional limitations discussed in Chapter 3.[239]

74.190 The ALRC acknowledges that this approach differs from the proposed model for reform of information privacy legislation relating to the state and territory public sectors discussed in Chapter 3. The difference is warranted, however, because the handling of personal information is currently regulated in all state and territory public sectors. As no states or territories currently have a statutory cause of action for invasion of privacy, failure to extend the coverage of the cause of action to state and territory public sectors would result in gaps in coverage, rather than merely inconsistent regulation.

74.191 If, however, states and territories adopted mirror legislation enacting the cause of action, or a cooperative scheme to regulate state and territory public sectors,[240] then there would be no need for the federal legislation to cover the state and territory public sectors. It is important to ensure that a consistent regime is enacted—how precisely that is achieved is a matter for government.

Should the statutory cause of action be in the *Privacy Act*?

74.192 The prevailing view of supporters of a cause of action for invasion of privacy is that the cause of action should be enacted in federal legislation. In response to IP 31, the OPC suggested that the role, if any, to be played by the Privacy Commissioner should determine the location of the cause of action.

> If the tort is actionable via the complaints process administered by the Privacy Commissioner, then there may be merit in streamlining all privacy-related complaints through this process. By contrast, if the tort will be actionable directly in the Courts it may be preferable to create a separate statute, to distinguish the tort of invasion of privacy from complaints handled under the Privacy Act.[241]

74.193 The recommended cause of action for invasion of privacy extends beyond information privacy, which is the current focus of the *Privacy Act*. Disclosure of personal information, however, may give rise to both a breach of the privacy principles and liability under the cause of action. Conversely, adherence to guidelines issued by the OPC, or protocols designed to ensure compliance with privacy principles, may be a relevant factor in determining whether the privacy principles have been breached, or the elements of the cause of action made out.

---

239 The distinction between federal, state and territory agencies is discussed in detail in Ch 34.
240 See Ch 3.
241 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

74.194 The same circumstances, therefore, may give rise to a complaint to the Privacy Commissioner under the *Privacy Act*, and an action in court for invasion of privacy. While the statute could provide that an individual must choose either to lodge a complaint or institute a cause of action, the ALRC considers that such a requirement is undesirable. An individual should be able to choose the forum that will provide the most appropriate remedy. The costs associated with pursuing the action or complaint also will be a relevant factor. Further, if pursuing both avenues simultaneously can be shown to be unfair, the proceedings in one forum may be stayed pending the outcome in the other forum.[242]

74.195 In DP 72, the ALRC's preliminary view was that the *Privacy Act* should be amended to include a new part setting out the provisions relating to the cause of action for a serious invasion of privacy. However, the ALRC now takes the view that there may be significant confusion arising from the placement of the cause of action in that Act. For example, whether the exemptions under the *Privacy Act* applied to the cause of action, and the interaction between the cause of action and other complaint mechanisms, may be unclear if the *Privacy Act* were amended to include the cause of action. The ALRC therefore recommends that the cause of action should be enacted in a separate federal statute. The legislation should abolish any common law action for the invasion or violation of a person's privacy.

74.196 A related, but separate, question is whether the appropriate forum to bring the action is the state and territory or federal courts. Locating the cause of action in federal legislation does not preclude state courts from hearing such matters. The use of state courts to hear federal matters is made possible by ss 71 and 77(iii) of the *Australian Constitution*. Section 71 vests the judicial power of the Commonwealth in the High Court, in such other federal courts as the Australian Parliament creates, and in such other courts as it invests with federal jurisdiction. Section 77(iii) provides that the Australian Parliament may make laws investing state courts with federal jurisdiction. Section 39(2) of the *Judiciary Act 1903* (Cth) invests state courts with federal jurisdiction in both civil and criminal matters, subject to certain limitations and exceptions.[243]

74.197 The appropriate court to hear the action will depend on the circumstances giving rise to liability, and the nature and extent of the remedies claimed. If the cases brought to date in Australia are any guide, it is likely that the district and county courts will be the most appropriate forum given the scope of their jurisdiction, the cost of litigating in those courts, and the expertise of the judges in hearing comparable matters, such as tort actions.

---

242 For a discussion of the power of a court to grant a stay, see *Walton v Gardiner* (1993) 177 CLR 380, 392–393; S Odgers, *Uniform Evidence Law* (6th ed, 2004), [1.1.1240]–[1.1.1260]. For a discussion of the complaint-handling powers of the OPC, see Ch 49.

243 See Australian Law Reform Commission, *The Judicial Power of the Commonwealth*, ALRC 92 (2001).

74.198 It is important that the general public be informed about activities that may give rise to liability under the cause of action, including the possible consequences of publishing material on the internet.[244] The ALRC recommends that the OPC provide information to the public concerning the recommended statutory cause of action. This is consistent with the Privacy Commissioner's oversight and educational functions under s 27 of the *Privacy Act.*

Recommendation 74–1 Federal legislation should provide for a statutory cause of action for a serious invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, a serious invasion of privacy may occur where:

(a) there has been an interference with an individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

(d) sensitive facts relating to an individual's private life have been disclosed.

Recommendation 74–2 Federal legislation should provide that, for the purpose of establishing liability under the statutory cause of action for invasion of privacy, a claimant must show that in the circumstances:

(a) there is a reasonable expectation of privacy; and

(b) the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

In determining whether an individual's privacy has been invaded for the purpose of establishing the cause of action, the court must take into account whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression).

244 See S Hawkins, *Submission PR 382*, 6 December 2007.

Recommendation 74–3 Federal legislation should provide that an action for a serious invasion of privacy:

(a) may only be brought by natural persons;

(b) is actionable without proof of damage; and

(c) is restricted to intentional or reckless acts on the part of the respondent.

Recommendation 74–4 The range of defences to the statutory cause of action for a serious invasion of privacy provided for in federal legislation should be listed exhaustively. The defences should include that the:

(a) act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(b) act or conduct was required or authorised by or under law; or

(c) publication of the information was, under the law of defamation, privileged.

Recommendation 74–5 To address a serious invasion of privacy, the court should be empowered to choose the remedy that is most appropriate in the circumstances, free from the jurisdictional constraints that may apply to that remedy in the general law. For example, the court should be empowered to grant any one or more of the following:

(a) damages, including aggravated damages, but not exemplary damages;

(b) an account of profits;

(c) an injunction;

(d) an order requiring the respondent to apologise to the claimant;

(e) a correction order;

(f) an order for the delivery up and destruction of material; and

(g) a declaration.

Recommendation 74–6 Federal legislation should provide that any action at common law for invasion of a person's privacy should be abolished on enactment of these provisions.

Recommendation 74–7 The Office of the Privacy Commissioner should provide information to the public concerning the recommended statutory cause of action for a serious invasion of privacy.

Appendix 1. List of Submissions

Name	*Submission Number*	*Date*
AAMI	PR 147	29 January 2007
AAPT Ltd	PR 87	15 January 2007
AAPT Ltd	PR 260	20 March 2007
AAPT Ltd	PR 338	7 November 2007
Abacus–Australian Mutuals	PR 174	6 February 2007
Abacus–Australian Mutuals	PR 278	10 April 2007
Abacus–Australian Mutuals	PR 456	11 December 2007
ACT Department of Justice and Community Safety	PR 577	12 March 2008
ACT Government Department of Disability Housing and Community Services	PR 495	19 December 2007
ACTU	PR 155	31 January 2007
Acxiom	PR 551	1 January 2008
J Adams	PR 204	21 February 2007
Administrative Appeals Tribunal	PR 201	20 February 2007
Administrative Appeals Tribunal	PR 481	17 December 2007
Adoption Privacy Protection Group Incorporated	PR 116	15 January 2007
AFL Players' Association	PR 393	7 December 2007
S Akgul	PR 380	6 December 2007

Name	***Submission Number***	***Date***
Alacrity Technologies	PR 348	23 November 2007
S Alexander	PR 51	18 August 2006
American Express	PR 257	16 March 2007
R Anderson	PR 373	4 December 2007
Anglicare Tasmania	PR 135	19 January 2007
Anglicare Tasmania	PR 514	21 December 2007
Anonymous	PR 22	20 June 2006
Anonymous	PR 175	6 February 2007
Anonymous	PR 181	6 January 2007
Anonymous	PR 189	10 February 2007
Anonymous	PR 194	8 February 2007
Anonymous	PR 241	9 March 2007
Anonymous	PR 243	8 March 2007
Anonymous	PR 244	8 March 2007
Anonymous	PR 248	8 March 2007
Anonymous	PR 249	8 March 2007
Anonymous	PR 250	8 March 2007
Anonymous	PR 253	10 February 2007
Anonymous	PR 267	24 March 2007
Anonymous	PR 279	29 March 2007
Anonymous	PR 280	3 April 2007
Anonymous	PR 283	12 April 2007

Name	***Submission Number***	***Date***
Anonymous	PR 328	1 October 2007
D Antulov	PR 14	28 May 2006
ANZ	PR 173	6 February 2007
ANZ	PR 291	10 May 2007
ANZ	PR 467	13 December 2007
Arts Law Centre of Australia	PR 125	15 January 2007
Arts Law Centre of Australia	PR 450	7 December 2007
Artsource	PR 350	28 November 2007
Association of Market and Social Research Organisations and Australian Market and Social Research Society	PR 502	20 December 2007
ASTRA	PR 426	7 December 2007
AUSTRAC	PR 216	1 March 2007
Australia Post	PR 78	10 January 2007
Australia Post	PR 445	10 December 2007
Australia's National Computer Emergency Response Team	PR 474	14 December 2007
Australasian Compliance Institute	PR 102	15 January 2007
Australasian Compliance Institute	PR 419	7 December 2007
Australasian Epidemiological Association	PR 473	14 December 2007
Australasian Retail Credit Association	PR 218	7 March 2007
Australasian Retail Credit Association	PR 352	29 November 2007
Australian Bankers' Association Inc	PR 259	19 March 2007

Name	***Submission Number***	***Date***
Australian Bankers' Association Inc	PR 567	11 February 2008
Australian Broadcasting Corporation	PR 94	15 January 2007
Australian Broadcasting Corporation	PR 571	18 February 2008
Australian Bureau of Statistics	PR 96	15 January 2007
Australian Bureau of Statistics	PR 383	6 December 2007
Australian Business Industrial	PR 444	10 December 2007
Australian Chamber of Commerce and Industry	PR 219	7 March 2007
Australian Chamber of Commerce and Industry	PR 452	7 December 2007
Australian Collectors Association	PR 505	20 December 2007
Australian Commission for Law Enforcement Integrity	PR 449	11 December 2007
Australian Commission on Safety and Quality in Health Care	PR 252	14 March 2007
Australian Communications and Media Authority	PR 268	26 March 2007
Australian Communicaitons and Media Authority	PR 522	21 December 2007
Australian Competition and Consumer Commission	PR 178	31 January 2007
Australian Competition and Consumer Commission	PR 437	10 December 2007
Australian Credit Forum	PR 492	19 December 2007
Australian Digital Alliance	PR 422	7 December 2007
Australian Direct Marketing Association	PR 298	29 June 2007

Name	***Submission Number***	***Date***
Australian Direct Marketing Association	PR 543	21 December 2007
Australian Electrical and Electronic Manufacturers' Association	PR 124	15 January 2007
Australian Federal Police	PR 186	9 February 2007
Australian Federal Police	PR 545	24 December 2007
Australian Finance Conference	PR 294	18 May 2007
Australian Finance Conference	PR 398	7 December 2007
Australian Government Attorney-General's Department	PR 546	24 December 2007
Australian Government Centrelink	PR 555	21 December 2007
Australian Government Department of Agriculture, Fisheries and Forestry	PR 556	7 Jaunary 2008
Australian Government Department of Broadband, Communications and the Digital Economy	PR 512	21 December 2007
Australian Government Department of Communications, Information Technology and the Arts	PR 264	22 March 2007
Australian Government Department of Defence	PR 440	10 December 2007
Australian Government Department of Employment and Workplace Relations	PR 211	27 February 2007
Australian Government Department of Families, Community Services and Indigenous Affairs	PR 162	31 January 2007

Name	***Submission Number***	***Date***
Australian Government Department of Families, Housing, Community Services and Indigenous Affairs	PR 559	15 January 2008
Australian Government Department of Finance and Deregulation	PR 558	11 January 2008
Australian Government Department of Foreign Affairs and Trade	PR 563	24 January 2008
Australian Government Department of Health and Ageing	PR 273	30 March 2007
Australian Government Department of Human Services	PR 136	19 January 2007
Australian Government Department of Human Services	PR 541	21 December 2007
Australian Government Treasury	PR 581	20 March 2008
Australian Guardianship and Administration Committee	PR 129	17 January 2007
Australian Guardianship and Administration Committee	PR 560	17 January 2008
Australian Health Insurance Association	PR 161	31 January 2007
Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association	PR 494	19 December 2007
Australian Information Industry Association	PR 410	7 December 2007
Australian Institute of Company Directors	PR 424	7 December 2007
Australian Institute of Credit Management	PR 224	9 March 2007
Australian Institute of Criminology	PR 461	12 December 2007
Australian Institute of Health and Welfare	PR 170	5 February 2007

Name	***Submission Number***	***Date***
Australian Institute of Health and Welfare	PR 552	2 January 2008
Australian Investigators Association Ltd	PR 507	21 December 2007
Australian Labor Party	PR 486	18 December 2007
Australian Lawyers Alliance	PR 528	21 December 2007
Australian Library and Information Association	PR 446	10 December 2007
Australian Medical Association	PR 524	21 December 2007
Australian Mercantile Agents Association	PR 508	21 December 2007
Australian Mobile Telecommunications Association	PR 154	30 January 2007
Australian Network for Art and Technology	PR 434	10 December 2007
Australian Nuclear Veterans Association Inc	PR 324	24 September 2007
Australian Nursing Federation	PR 205	22 February 2007
Australian Press Council	PR 48	8 August 2006
Australian Press Council	PR 83	12 January 2007
Australian Press Council	PR 411	7 December 2007
Australian Privacy Foundation	PR 167	2 February 2007
Australian Privacy Foundation	PR 275	2 April 2007
Australian Privacy Foundation	PR 553	2 January 2008
Australian Professional Footballers' Association	PR 430	10 December 2007
Australian Retailers Association	PR 131	18 January 2007
Australian Security Intelligence Organisation	PR 180	9 February 2007

Name	***Submission Number***	***Date***
Australian Society of Archivists	PR 460	11 December 2007
Australian Taxation Office	PR 168	15 February 2007
Australian Taxation Office	PR 515	21 December 2007
Australian Unity Group	PR 381	6 December 2007
Avant Mutual Group Ltd	PR 421	7 December 2007
AXA	PR 119	15 January 2007
AXA	PR 442	10 December 2007
P Baird	PR 584	10 April 2008
Banking and Financial Services Ombudsman Ltd	PR 263	21 March 2007
Banking and Financial Services Ombudsman Ltd	PR 370	4 December 2007
Banking and Financial Services Ombudsman Ltd	PR 471	14 December 2007
M Bartucciotto	PR 62	27 November 2006
P Baum	PR 34	1 June 2006
A Baxter	PR 74	5 January 2007
L Bennett	PR 21	11 June 2006
B Bhoola	PR 314	25 August 2007
R Blunden	PR 262	15 March 2007
D Boesel	PR 117	15 January 2007
J Boggs	PR 245	8 March 2007
J Bogotto	PR 140	23 January 2006

Name	***Submission Number***	***Date***
K Bottomley	PR 10	1 May 2006
D Bowman	PR 330	19 October 2007
BPay	PR 566	31 January 2008
N Bradley	PR 573	22 February 2008
K Breen	PR 578	13 March 2008
C Brice	PR 337	1 November 2007
S Bronitt, J Stellios and K Leong	PR 213	27 February 2007
BUPA Australia Health	PR 455	7 December 2007
Business Loans Australia Pty Ltd	PR 282	16 April 2007
L Bygrave	PR 92	15 January 2007
CadWest	PR 511	21 December 2007
W Caelli	PR 99	15 January 2007
L Callahan	PR 276	2 April 2007
G Campbell	PR 54	9 October 2006
Cancer Council of Australia and Clinical Oncological Society of Australia	PR 544	23 December 2007
Care Leavers Australia Nework	PR 266	23 March 2007
Carers Australia	PR 423	7 December 2007
J Carland and J Pagan	PR 42	11 July 2006
Caroline Chisholm Centre for Health Ethics	PR 69	24 December 2006
R Carroll	PR 550	29 December 2007
Centre for Law and Genetics	PR 127	16 January 2007

Name	***Submission Number***	***Date***
Centre for Law and Genetics	PR 497	20 December 2007
Chartered Secretaries Australia	PR 351	28 November 2007
Chocolate Messages Pty Ltd	PR 9	1 June 2006
F Churcher	PR 240	9 March 2007
Citibank Pty Ltd	PR 428	7 December 2007
Civil Liberties Australia	PR 98	15 January 2007
Civil Liberties Australia	PR 469	14 December 2007
P Coad	PR 121	15 January 2007
J Codrington	PR 81	2 January 2007
D Collins	PR 369	4 December 2007
Commonwealth Bank	PR 392	7 December 2007
Commonwealth Ombudsman	PR 202	21 February 2007
Communications Alliance Ltd	PR 198	16 February 2007
Communications Alliance Ltd	PR 439	10 December 2007
Community Services Ministers' Advisory Council	PR 47	28 July 2006
Confidential	PR 5	3 April 2006
Confidential	PR 6	6 March 2006
Confidential	PR 13	26 May 2006
Confidential	PR 24	6 June 2006
Confidential	PR 27	4 June 2006
Confidential	PR 31	3 June 2006

Name	***Submission Number***	***Date***
Confidential	PR 32	2 June 2006
Confidential	PR 49	14 August 2006
Confidential	PR 50	15 August 2006
Confidential	PR 60	27 November 2006
Confidential	PR 88	15 January 2007
Confidential	PR 97	15 January 2007
Confidential	PR 130	17 January 2007
Confidential	PR 132	18 January 2007
Confidential	PR 134	19 January 2007
Confidential	PR 143	24 January 2007
Confidential	PR 165	1 February 2007
Confidential	PR 179	8 February 2007
Confidential	PR 188	9 February 2007
Confidential	PR 206	22 February 2007
Confidential	PR 214	27 February 2007
Confidential	PR 223	8 March 2007
Confidential	PR 227	9 March 2007
Confidential	PR 261	17 March 2007
Confidential	PR 297	1 June 2007
Confidential	PR 312	22 August 2007
Confidential	PR 319	13 September 2007

Name	***Submission Number***	***Date***
Confidential	PR 326	28 September 2007
Confidential	PR 327	28 September 2007
Confidential	PR 332	19 October 2007
Confidential	PR 340	4 November 2007
Confidential	PR 356	2 December 2007
Confidential	PR 374	5 December 2007
Confidential	PR 376	5 December 2007
Confidential	PR 377	5 December 2007
Confidential	PR 399	7 December 2007
Confidential	PR 431	10 December 2007
Confidential	PR 448	11 December 2007
Confidential	PR 488	19 December 2007
Confidential	PR 513	21 December 2007
Confidential	PR 517	21 December 2007
Confidential	PR 519	21 December 2007
Confidential	PR 529	21 December 2007
Confidential	PR 535	21 December 2007
Confidential	PR 536	21 December 2007
Confidential	PR 570	13 February 2008
Confidential	PR 583	9 April 2008
J Connor	PR 239	9 March 2007
Consumer Action Law Centre	PR 274	2 April 2007

Name	***Submission Number***	***Date***
Consumer Action Law Centre	PR 510	21 December 2007
Consumer Credit Legal Centre (NSW) Inc	PR 28	6 June 2006
Consumer Credit Legal Centre (NSW) Inc	PR 160	31 January 2007
Consumer Credit Legal Centre (NSW) Inc	PR 255	16 March 2007
Contemporary Arts Organisations Australia	PR 384	6 December 2007
M Cook	PR 453	7 December 2007
C Copeland	PR 301	28 June 2007
Council of Small Business of Australia	PR 389	6 December 2007
Council of Small Business Organisations of Australia Ltd	PR 203	21 February 2007
Council of Social Service of New South Wales	PR 115	15 January 2007
E Cousins	PR 585	11 April 2008
K M Corke and Associates	PR 447	10 December 2007
CPA Australia	PR 476	14 December 2007
CrimTrac	PR 158	31 January 2007
S Crothers	PR 43	14 July 2006
S Crothers	PR 77	8 January 2007
S Crowe	PR 234	2 March 2007
CSIRO	PR 176	6 February 2007
I Cunliffe	PR 37	9 May 2006
Cyberspace Law and Policy Centre UNSW	PR 487	19 December 2007

Name	***Submission Number***	***Date***
T de Koke	PR 8	5 April 2006
G Dean	PR 331	15 October 2007
Department of Health Western Australia	PR 139	23 January 2006
DLA Phillips Fox	PR 111	15 January 2007
W Dowdell	PR 1	16 February 2006
J Dowse	PR 44	2 June 2006
J Drake-Brockman	PR 311	17 August 2007
Dun & Bradstreet (Australia) Pty Ltd	PR 11	13 April 2006
Dun & Bradstreet (Australia) Pty Ltd	PR 232	9 March 2007
Dun & Bradstreet (Australia) Pty Ltd	PR 401	7 December 2007
Edentiti	PR 29	3 June 2006
Edentiti	PR 210	27 February 2007
Electronic Frontiers Australia Inc	PR 76	8 January 2007
Energy and Water Ombudsman NSW	PR 225	9 March 2007
EnergyAustralia	PR 229	9 March 2007
O Esmonde-Morgan	PR 361	3 December 2007
Experian Asia Pacific	PR 228	9 March 2007
Family Law Council	PR 269	28 March 2007
FCS OnLine	PR 441	10 December 2007
Federation of Community Legal Centres (Vic)	PR 509	21 December 2007
M Fenotti	PR 86	15 January 2007

Name	***Submission Number***	***Date***
Festival of Light Australia	PR 354	1 December 2007
Finance Sector Union	PR 109	15 January 2007
Financial Counsellors Association of Queensland	PR 371	30 November 2007
Financial Planning Association of Australia	PR 496	19 December 2007
First Data International	PR 503	20 December 2007
H Fisher	PR 582	31 March 2008
R Fitzpatrick	PR 315	8 September 2007
H Fleming	PR 38	27 June 2006
B Fletcher	PR 296	29 May 2007
Foreign Intelligence Agencies of the Australian Intelligence Community	PR 159	31 January 2007
Foreign Intelligence Agencies of the Australian Intelligence Community	PR 466	13 December 2007
Free TV Australia	PR 149	29 January 2007
Fundraising Institute–Australia Ltd	PR 138	22 January 2007
Galexia Pty Ltd	PR 465	13 December 2007
K Gardiner	PR 33	1 June 2006
GE Money Australia	PR 233	12 March 2007
GE Money Australia	PR 537	21 December 2007
General Ethical Issues Sub-Committee—Alfred Hospital Ethics Committee	PR 192	15 February 2007
General Ethical Issues Sub-Committee—	PR 531	21 December 2007

Name	***Submission Number***	***Date***
Alfred Hospital Ethics Committee		
K Gibbons	PR 464	13 December 2007
Justice G Giudice	PR 91	15 January 2007
Global Data Company	PR 409	7 December 2007
Google Australia	PR 539	21 December 2007
N Gordon	PR 75	7 January 2007
K Goss	PR 391	6 December 2007
Government of South Australia	PR 187	12 February 2007
Government of South Australia	PR 565	29 January 2008
Government of Victoria	PR 288	26 April 2007
I Graham	PR 427	9 December 2007
G Grantham	PR 576	3 March 2008
G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW	PR 183	9 February 2007
N Griffiths	PR 395	7 December 2007
D Hall	PR 61	27 November 2006
D Hall	PR 372	4 December 2007
E Halvorson	PR 367	3 December 2007
D Hamilton	PR 30	5 June 2006
P Hammer	PR 396	7 December 2007
K Handscombe	PR 52	18 September 2006
K Handscombe	PR 89	15 January 2007
Rev B Harris	PR 321	14 September 2007

Name	***Submission Number***	***Date***
J Harvey	PR 12	25 May 2006
S Hawkins	PR 382	6 December 2007
HBOS Australia	PR 475	14 December 2007
Health and Community Services Complaints Commission (South Australia)	PR 207	23 February 2007
Health Informatics Society of Australia	PR 196	16 January 2007
Health Informatics Society of Australia	PR 554	2 January 2008
T Higgins	PR 191	14 February 2007
D Hill	PR 335	26 October 2007
Hobart Branch of National Seniors Association Ltd	PR 368	4 December 2007
B Hogan	PR 362	2 December 2007
HSBC	PR 417	7 December 2007
A Hugo	PR 285	19 April 2007
Human Rights and Equal Opportunity Commission	PR 500	20 December 2007
Human Variome Project	PR 287	23 April 2007
M Hunter	PR 16	1 June 2006
IBM Australia	PR 405	7 December 2007
Industry Based Alternative Dispute Resolution Schemes, joint submission	PR 93	15 January 2007
ING Bank (Australia) Limited	PR 230	9 March 2007
ING Bank (Australia) Limited	PR 420	7 December 2007

Name	***Submission Number***	***Date***
Insolvency and Trustee Service Australia	PR 123	15 January 2007
Insolvency and Trustee Service Australia	PR 235	12 March 2007
Insolvency Practitioners Association	PR 404	7 December 2007
Inspector-General of Intelligence and Security	PR 432	10 December 2007
Institute of Mercantile Agents	PR 101	15 January 2007
Institute of Mercantile Agents	PR 270	28 March 2007
Insurance Council of Australia	PR 110	15 January 2007
Insurance Council of Australia	PR 485	18 December 2007
Investment and Financial Services Association	PR 122	15 January 2007
Investment and Financial Services Association	PR 538	21 December 2007
A Jackson	PR 142	24 January 2007
A Jackson	PR 289	26 April 2007
S Jefferies	PR 295	28 May 2007
A Johnston	PR 70	31 December 2006
A Johnston	PR 251	8 March 2007
M Johnston	PR 342	16 November 2007
D Jones	PR 341	15 November 2007
N Keele	PR 53	9 October 2006
J Kerr	PR 4	13 March 2006
J Kerr	PR 63	28 November 2006

Name	***Submission Number***	***Date***
T Kerr	PR 309	5 August 2007
J Keys	PR 358	2 December 2007
B Laing	PR 339	12 November 2007
R Lake	PR 305	19 July 2007
S Lake	PR 347	23 November 2007
A Lamb	PR 157	31 January 2007
M Lander	PR 58	7 November 2006
M Lander	PR 190	14 February 2007
M Lander	PR 238	9 March 2007
M Lander	PR 451	7 December 2007
Law Council of Australia	PR 177	8 February 2007
Law Council of Australia	PR 527	21 December 2007
Law Institute of Victoria	PR 200	21 February 2007
Law Society of New South Wales	PR 146	29 January 2007
Law Society of New South Wales	PR 443	10 December 2007
Layton Technology Pty Ltd	PR 562	24 January 2008
P Lee-Archer	PR 20	2 June 2006
Legal Aid Commission of New South Wales	PR 107	15 January 2007
Legal Aid Queensland	PR 212	27 February 2007
Legal Aid Queensland	PR 292	11 May 2007
Legal Aid Queensland	PR 489	19 December 2007

Name	***Submission Number***	***Date***
Liberty Victoria—Victorian Council for Civil Liberties	PR 540	21 December 2007
Link Market Service	PR 2	24 February 2006
L Lucas	PR 95	15 January 2007
R Lucienne	PR 477	16 December 2007
A Lyons	PR 290	30 April 2007
M Lyons and B Le Plastrier	PR 41	11 July 2006
R Magnusson	PR 3	9 March 2006
M Maguire	PR 18	1 June 2006
P Maindonald	PR 90	15 January 2007
Mastercard Worldwide	PR 237	13 March 2007
Mastercard Worldwide	PR 425	7 December 2007
B McCarthy	PR 579	19 March 2008
Media Entertainment and Arts Alliance	PR 406	7 December 2007
Medicare Australia	PR 534	21 December 2007
D Meehan	PR 345	22 November 2007
Mental Health Legal Centre Inc	PR 184	1 February 2007
MGIC Australia	PR 479	17 December 2007
Microsoft Asia Pacific	PR 463	12 December 2007
Microsoft Australia	PR 113	15 January 2007
Midena Lawyers	PR 363	3 December 2007
Migration Review Tribunal and Refugee Review Tribunal	PR 126	16 January 2007

Name	***Submission Number***	***Date***
Migration Review Tribunal and Refugee Review Tribunal	PR 533	21 December 2007
R Minahan	PR 482	13 December 2007
Min-it Software	PR 236	13 March 2007
L Mitchell	PR 46	2 June 2006
M Moore	PR 307	3 August 2007
M Monroe	PR 320	13 September 2007
Mortgage and Finance Association of Australia	PR 231	9 March 2007
Mortgage and Finance Association of Australia	PR 344	19 November 2007
J Mortelliti	PR 357	2 December 2007
Motor Traders Association of NSW	PR 429	10 December 2007
Motor Trades Association of Australia	PR 470	14 December 2007
National Alternative Dispute Resolution Advisory Council	PR 564	23 January 2008
National Archives of Australia	PR 199	20 February 2007
National Archives of Australia	PR 414	7 December 2007
National Association for Information Destruction	PR 133	19 January 2007
National Association for Information Destruction (Australasia)	PR 483	17 December 2007
National Association for the Visual Arts Ltd	PR 151	30 January 2007
National Association for the Visual Arts Ltd	PR 415	7 December 2007

Name	***Submission Number***	***Date***
National Australia Bank	PR 408	7 December 2007
National Australia Bank and MLC Ltd	PR 148	29 January 2007
National Catholic Education Commission and Independent Schools Council of Australia	PR 85	12 January 2007
National Catholic Education Commission and Independent Schools Council of Australia	PR 462	12 December 2007
National Children's and Youth Law Centre	PR 166	1 February 2007
National Children's and Youth Law Centre	PR 491	19 December 2007
National Credit Union Association Inc	PR 226	9 March 2007
National E-health Transition Authority	PR 145	29 January 2007
National Health and Medical Research Council	PR 114	15 January 2007
National Health and Medical Research Council	PR 397	7 December 2007
National Legal Aid	PR 265	23 March 2007
National Legal Aid	PR 521	21 December 2007
National Native Title Tribunal	PR 402	7 December 2007
National Prescribing Service	PR 547	24 December 2007
National Relay Service	PR 484	18 December 2007
National and State Libraries Australasia	PR 68	21 December 2006
National Transport Commission	PR 416	7 December 2007
New South Wales Aboriginal Justice Advisory Council	PR 501	20 December 2007
New South Wales Council for Civil Liberties Inc	PR 156	31 January 2007

Name	***Submission Number***	***Date***
New South Wales Department of Corrective Services	PR 561	23 January 2008
New South Wales Government Department of Health	PR 458	11 December 2007
New South Wales Guardianship Tribunal	PR 209	23 February 2007
New South Wales Guardianship Tribunal	PR 403	7 December 2007
New South Wales Office of the Protective Commissioner	PR 516	21 December 2007
New Zealand Privacy Commissioner	PR 128	17 January 2007
S Newton	PR 23	8 June 2006
P Nolan	PR 322	16 September 2007
Northern Territory Government Department of Health and Community Services	PR 480	17 December 2007
NSW Commission for Children and Young People	PR 120	15 January 2007
NSW Disability Discrimination Legal Centre (Inc)	PR 105	16 January 2007
S Nyman	PR 303	18 July 2007
Obesity Policy Coalition	PR 506	20 December 2007
Obesity Prevention Policy Coalition and Young Media Australia	PR 144	25 January 2007
L O'Connor	PR 35	2 June 2006
C O'Donnell	PR 57	23 October 2006
C O'Donnell	PR 73	5 January 2007

Name	***Submission Number***	***Date***
Office of the Health Services Commissioner (Victoria)	PR 153	30 January 2007
Office of the Health Services Commissioner (Victoria)	PR 518	21 December 2007
Office of the Information Commissioner (Northern Territory)	PR 103	15 January 2007
Office of the Privacy Commissioner	PR 215	28 February 2007
Office of the Privacy Commissioner	PR 281	13 April 2007
Office of the Privacy Commissioner	PR 499	20 December 2007
Office of the Public Advocate Queensland	PR 195	12 February 2007
Office of the Public Advocate Queensland	PR 435	10 December 2007
Office of the Public Advocate Victoria	PR 141	24 January 2007
Office of the Victorian Privacy Commissioner	PR 217	28 February 2007
Office of the Victorian Privacy Commissioner	PR 493	19 December 2007
Q O'Keefe	PR 182	19 January 2007
Optus	PR 258	16 March 2007
Optus	PR 532	21 December 2007
E Orr	PR 346	22 November 2007
H Page	PR 360	2 December 2007
P Parker	PR 304	19 July 2007
J Partridge	PR 26	4 June 2006
Pharmacy Guild of Australia	PR 433	10 December 2007

Name	***Submission Number***	***Date***
F Pilcher	PR 17	1 June 2006
PMI Mortgage Insurance Ltd	PR 412	7 December 2007
Police Federation of Australia	PR 293	14 May 2007
Police Federation of Australia	PR 385	6 December 2007
T Pollington	PR 318	13 September 2007
G Poscoliero	PR 575	3 March 2008
K Pospisek	PR 104	15 January 2007
Privacy NSW	PR 193	15 February 2007
Privacy NSW	PR 468	14 December 2007
Public Interest Advocacy Centre	PR 548	26 December 2007
Public Record Office Victoria	PR 72	3 January 2007
K Purcell	PR 359	2 December 2007
Pureprofile	PR 526	21 December 2007
Queensland Council for Civil Liberties	PR 150	29 January 2007
Queensland Goverment	PR 242	15 March 2007
Queensland Government	PR 490	19 December 2007
Queensland Government Commission for Children and Young People and Child Guardian	PR 171	5 February 2007
Queensland Institute of Medical Research	PR 80	11 January 2007
Queensland Law Society	PR 286	20 April 2007
Queensland Police Service	PR 222	9 March 2007

Name	***Submission Number***	***Date***
Recruitment and Consulting Services Association Australia & New Zealand	PR 353	30 November 2007
Real Estate Institute of Australia	PR 7	10 April 2006
Real Estate Institute of Australia	PR 84	12 January 2007
Real Estate Institute of Australia	PR 400	7 December 2007
W Realph	PR 208	27 February 2007
W Realph	PR 386	6 December 2007
T Reardon	PR 306	31 July 2007
B Regan	PR 387	6 December 2007
Retail Motor Industry	PR 407	7 December 2007
K Richards	PR 308	2 August 2007
M Rickard	PR 19	1 June 2006
Right to Know Coalition	PR 542	21 December 2007
M Rimmer	PR 379	5 December 2007
S Rowney	PR 316	10 September 2007
Royal Women's Hospital Melbourne	PR 108	15 January 2007
H Ruglen	PR 39	27 June 2006
Salvation Army	PR 15	2 June 2006
R Sands	PR 317	12 September 2007
SBS	PR 112	15 January 2007
M Schaefer	PR 364	3 December 2007
School of Public Health—University of Sydney	PR 504	20 December 2007

Name	***Submission Number***	***Date***
N Sertori	PR 349	23 November 2007
H Shaud	PR 366	4 December 2007
L Sigal	PR 549	29 December 2007
J Simpson	PR 336	29 October 2007
P Slatterie	PR 329	3 October 2007
P Smart	PR 323	23 September 2007
Smartnet	PR 457	11 December 2007
A Smith	PR 79	2 January 2007
K Smith	PR 246	8 March 2007
T Smith	PR 325	14 September 2007
Social Security Appeals Tribunal	PR 106	15 January 2007
Social Security Appeals Tribunal	PR 478	17 December 2007
Special Broadcasting Service	PR 530	21 December 2007
St George Banking Limited	PR 271	29 March 2007
R Stinson	PR 247	8 March 2007
D Stones	PR 355	1 December 2007
T Stutt and L Nicholls	PR 40	11 July 2006
B Such	PR 71	2 January 2007
Suncorp-Metway Ltd	PR 525	21 December 2007
Tasmanian Collection Service	PR 375	5 Deceember 2007
Tasmanian Government Department of Health and Human Services	PR 436	10 December 2007

Name	***Submission Number***	***Date***
A Taylor	PR 56	26 October 2006
C Taylor	PR 36	17 June 2006
Telecommunications Industry Ombudsman	PR 221	8 March 2007
Telstra Corporation Limited	PR 185	9 February 2007
Telstra Corporation Limited	PR 459	11 December 2007
Tenants Union of NSW Co-op Ltd	PR 169	5 February 2007
Tenants Union of Victoria Ltd	PR 197	16 February 2007
The Herald and Weekly Times Pty Ltd	PR 568	11 February 2008
The Mailing House	PR 64	1 December 2006
L Thomas	PR 65	9 December 2006
L Thompson	PR 220	26 February 2007
C Thomson	PR 454	7 December 2007
W Tilly	PR 574	25 February 2008
A Tonking	PR 67	20 December 2006
J Tozzi-Condivi	PR 438	10 December 2007
S Tracey	PR 310	16 August 2007
S Tully	PR 25	7 June 2006
I Turnbull	PR 82	12 January 2007
I Turnbull	PR 378	5 December 2007
Uniform Consumer Credit Code Management Committee	PR 520	21 December 2007
Unisys	PR 569	12 February 2008

Name	***Submission Number***	***Date***
United Medical Protection	PR 118	15 January 2007
United Nations Youth Association, Flinders University Students' Association, Adelaide University Law Students' Society	PR 557	7 January 2008
University of Newcastle	PR 413	7 December 2007
University of Western Sydney Human Research Ethics Committee	PR 418	7 December 2007
R Varney	PR 333	22 October 2007
Veda Advantage	PR 163	31 January 2007
Veda Advantage	PR 272	29 March 2007
Veda Advantage	PR 498	20 December 2007
L Vella	PR 284	17 April 2007
Victoria Police	PR 523	21 December 2007
Victorian Automobile Chamber of Commerce	PR 100	15 January 2007
Victorian Society for Computers and the Law Inc	PR 137	22 January 2007
R Vlassis	PR 580	19 March 2008
P Wain	PR 365	3 December 2007
H Walker	PR 55	20 October 2006
R Ward	PR 254	8 March 2007
N Waters—Cyberspace Law and Policy Centre UNSW	PR 277	3 April 2007
A Watson	PR 313	22 August 2007

Name	***Submission Number***	***Date***
J Watts	PR 302	10 July 2007
K Wells	PR 572	20 February 2008
Westpac	PR 256	16 March 2007
Westpac	PR 472	14 December 2007
P Wikramanayake	PR 45	1 June 2006
A Williams	PR 300	28 June 2007
WinMagic Inc	PR 59	24 November 2006
K Wynn	PR 299	20 June 2007
K Young	PR 343	16 November 2007
P Youngman	PR 394	7 December 2007
Youth Affairs Council of Victoria Inc	PR 172	5 February 2007
Youth Affairs Council of Victoria Inc	PR 388	6 December 2007
Youthlaw	PR 152	30 January 2007
Youthlaw	PR 390	6 December 2007

Appendix 2. List of Agencies, Organisations and Individuals Consulted

Name	*Location*
AAPT	Sydney
Abacus–Australian Mutuals	Sydney
Aboriginal Interpreter Service	Darwin
Aboriginal Justice Advisory Council	Sydney
M Abrams, Privacy Consultant	Toronto
ACXIOM	Sydney
Administrative Appeals Tribunal	Sydney
J Alhadeff, Chief Privacy Officer, Oracle	Sydney
American Express	Melbourne
ANZ	Melbourne
Professor B Armstrong, Director of Research, Sydney Cancer Centre	Sydney
Australasian Compliance Institute	Sydney
Australasian Epidemiological Association	Melbourne
Australasian Retail Credit Association	Sydney/Melbourne
Australian Broadcasting Corporation	Sydney
Australian Bureau of Statistics	Canberra
Australian Centre for Independent Journalism	Sydney
Australian Chamber of Commerce and Industry	Canberra
Australian Commission for Law Enforcement Integrity	Canberra
Australian Commission on Safety and Quality in Health Care	Sydney
Australian Communications and Media Authority	Sydney
Australian Crime Commission	Sydney

Australian Direct Marketing Association	Sydney
Australian Electoral Commission	Canberra
Australian Federal Police	Canberra
Australian Federation of AIDS Organisations	Sydney
Australian Federation of Travel Agents	Sydney
Australian Finance Conference	Sydney
Australian General Practice Network	Canberra
Australian Government Attorney-General's Department	Canberra/Sydney
Australian Government Defence Signals Directorate	Canberra
Australian Government Department of Communications, Information Technology and the Arts	Sydney
Australian Government Department of Employment and Workplace Relations	Canberra
Australian Government Department of Families, Community Services and Indigenous Affairs	Canberra
Australian Government Department of Foreign Affairs and Trade	Canberra
Australian Government Department of Health and Ageing	Sydney
Australian Government Department of Human Services	Canberra
Australian Government Department of Industry, Tourism and Resources	Sydney
Australian Government Department of Prime Minister and Cabinet	Canberra
Australian Government Department of Veterans' Affairs	Canberra
Australian Government Office of Access Card	Canberra
Australian Government Office of Small Business	Canberra
Australian Government Treasury	Canberra
Australian Health Insurance Association	Canberra
Australian Institute of Administrative Law South Australian Chapter	Adelaide

Australian Institute of Health and Welfare	Canberra
Australian Institute of Private Detectives	Sydney
Australian Interactive Media Industry Association	Sydney
Australian Medical Association	Canberra
Australian Press Council	Sydney
Australian Privacy Foundation	Sydney
Australian Research Alliance for Children and Youth	Perth
Australian Research Council	Canberra
Australian Security Intelligence Organisation	Sydney
Australian Subscription Television and Radio Association	Sydney
Australian Taxation Office	Canberra
Austroads	Sydney
Bank of Queensland	Melbourne
Banking and Financial Services Ombudsman	Melbourne
BankWest	Melbourne
A Beatty, Mallesons Stephen Jacques	Sydney
Biometrics Institute	Canberra
Professor J Black, London School of Economics	Sydney
P Black, School of Law, Queensland University of Technology	Brisbane
Professor S Bronitt, Faculty of Law, Australian National University	Canberra
T Brookes, Blake Dawson Waldron	Sydney
K Burton, School of Law, Queensland University of Technology	Brisbane
Professor W Caelli, Faculty of Information Technology, Queensland University of Technology	Brisbane
T Calma, Aboriginal and Torres Strait Islander Social Justice Commissioner and Race Discrimination Commissioner	Sydney

Cancer Australia	Sydney
Cancer Council Victoria	Melbourne
Professor T Carney, Faculty of Law, University of Sydney	Sydney
Professor C Cartwright, Aged Services Learning and Research Collaboration, Southern Cross University	Coffs Harbour
Centre for Excellence in Child and Family Welfare	Melbourne
Centre for Law and Genetics	Hobart
Centre for Multicultural Youth Issues	Melbourne
Centrelink	Canberra
CHOICE	Sydney
Citibank	Melbourne
K Clark, Allens Arthur Robinson	Melbourne
Professor R Clarke, Xamax Consultancy	Canberra
Commonwealth Bank	Melbourne
Commonwealth Ombudsman	Canberra
Communications Alliance Ltd	Sydney
Community Child Care Association	Melbourne
Consumer Credit Legal Centre (NSW)	Sydney
Consumers' Telecommunications Network	Sydney
Credit Corp	Sydney
Professor P Croll, Faculty of Information Technology, Queensland University of Technology	Brisbane
M Crompton and R McKenzie, Information Integrity Solutions	Sydney
P Cullen, Chief Privacy Officer, Microsoft	Sydney
I Cunliffe, Norton White	Melbourne
K Curtis, Privacy Commissioner, Australia	Sydney
J Douglas-Stewart, Privacy Law Consulting Australia	Sydney
Dun & Bradstreet	Sydney

K Eastman, Barrister	Sydney
Electronic Frontiers Australia	Brisbane
Embarcadero Technologies	Sydney
Energy and Water Ombudsman New South Wales	Sydney
Fairfax Media Ltd	Sydney
Family Court of Australia	Sydney
Federal Court of Australia	Sydney
Federal Magistrates Court of Australia	Sydney
Professor B Fitzgerald, School of Law, Queensland University of Technology	Brisbane
Free TV Australia	Sydney
Galexia Consulting	Sydney
GE Commercial	Sydney
GE Money	Sydney/Melbourne
D Giles, Freehills	Sydney
GIO	Sydney
Professor G Greenleaf, Faculty of Law, University of New South Wales	Sydney
Health Consumers Alliance of South Australia	Adelaide
Health Consumers' Council of Western Australia	Perth
High Court of Australia	Sydney
Dr R Hil, School of Arts and Social Sciences, Southern Cross University	Coffs Harbour
G Hill, State Trustees	Melbourne
Hill and Knowlton	Sydney
Professor D Holman, School of Population Health, University of Western Australia	Perth

HSBC	Melbourne
T Hughes, Executive Director, International Association of Privacy Professionals	Sydney
Human Rights and Equal Opportunity Commission	Sydney
IBM	Sydney
IMS Health Asia	Sydney
Inspector-General of Intelligence and Security	Canberra
Institute of Mercantile Agents	Sydney
Insurance Council of Australia	Sydney
Investment and Financial Services Association	Sydney
Professor M Jackson, School of Accounting and Law, RMIT University	Melbourne
P Jones, Allens Arthur Robinson	Sydney
Justice M Kellam, Supreme Court of Victoria	Melbourne
J King-Christopher, Blake Dawson Waldron	Brisbane
KPMG	Sydney
Professor B Lane, School of Law, Queensland University of Technology	Brisbane
Law Council of Australia, Privacy Working Group	Sydney
Legal Aid New South Wales	Sydney
Legal Aid Queensland, Consumer Protection Unit	Brisbane
Dr D Lindsay, Faculty of Law, Monash University	Melbourne
The Link Youth Health Service	Hobard
D Loukidelis, Information and Privacy Commissioner for British Columbia	London
C Lowry, Financial Counsellor	Sydney
A MacRae, former member of the Taskforce on Reducing the Regulatory Burden on Business	Melbourne

Associate Professor R Magnusson, Law School, University of Sydney	Sydney
MasterCard Worldwide	Sydney
Media Entertainment and Arts Alliance	Sydney
Medicare Australia	Canberra
Menzies School of Health Research	Darwin
J Moore, Mallesons Stephen Jaques	Sydney
National Aboriginal and Islander Child Care	Melbourne
National Archives of Australia	Canberra
National Association of Information Destruction	Sydney
National Australia Bank	Melbourne
National Children's and Youth Law Centre	Sydney
National E-Health Transition Authority	Canberra
National Health and Medical Research Council	Melbourne
National Health and Medical Research Council Privacy Working Committee	Canberra
New South Wales Commission for Children and Young People	Sydney
New South Wales Consumer, Trader and Tenancy Tribunal	Sydney
New South Wales Council for Civil Liberties	Sydney
New South Wales Law Reform Commission	Sydney
New South Wales Ombudsman	Sydney
New Zealand Law Commission	Sydney/Wellington
News Ltd	Sydney
North Coast Area Health Service	Coffs Harbour
Office of the Information and Privacy Commissioner, Ontario	Toronto
Office of the Information Commissioner, Northern Territory	Darwin
Office of the New South Wales Privacy Commissioner	Sydney

Office of the Privacy Commissioner	Sydney
Office of the Public Advocate Queensland	Brisbane
Office of the Victorian Privacy Commissioner	Melbourne
Ombudsman Western Australia	Perth
Optus	Sydney/Melbourne
Dr C Parker, University of Melbourne	Melbourne
Parliament of Australia, Department of Parliamentary Services	Canberra
Parliament of Australia, Department of the House of Representatives	Canberra
Parliament of Australia, Department of the Senate	Canberra
C Parr, Allens Arthur Robinson	Sydney
Associate Professor M Paterson, Faculty of Law, Monash University	Melbourne
Pharmacy Guild of Australia	Sydney
Dr L Ponemon, Chairman, Ponemon Institute	Sydney
Privacy Commissioner, New Zealand	Wellington
Privacy Committee of South Australia	Adelaide
Privacy NSW, Office of the New South Wales Privacy Commissioner	Sydney
Public Health Association of Australia	Canberra
Public Interest Advocacy Centre	Sydney
QBE Insurance Group	Sydney
Queensland Government Commission for Children and Young People and Child Guardian	Brisbane
Queensland Government Department of Justice and Attorney-General	Brisbane
Queensland Health	Brisbane
Queensland State Archives	Sydney
Associate Professor M Richardson, Faculty of Law, University of Melbourne	Melbourne

Right to Know Coalition	Sydney
Sawtell Catholic Care of the Aged	Coffs Harbour
Special Broadcasting Service	Sydney
P Schaar, Chairman, EU Art. 29 Data Protection Working Party, and H Neil	London
Sensis Interactive	Sydney
Seven Network Ltd	Sydney
Shopfront Youth Legal Centre	Sydney
Professor Sivakumar, Indian Law Institute	Sydney
A Smith, Mallesons Stephen Jaques	Sydney
Solicitor-General of the Northern Territory	Darwin
Professor T Sourdin, School of Law, La Trobe University	Sydney
South Australian Government Department for Families and Communities	Adelaide
South Australian Government Department of Health	Adelaide
South Australian Government Department of the Premier and Cabinet, Social Inclusion Unit	Adelaide
St George Bank	Melbourne
Standards Australia	Sydney
Professor F Stanley, Executive Director, Australian Research Alliance for Children and Youth	Sydney/Melbourne
State Records Authority of New South Wales	Sydney
State Records of South Australia	Adelaide
State Records Office of Western Australia	Perth
State Solicitor's Office Western Australia	Perth
Mr J Stellios, Faculty of Law, Australian National University	Canberra
J Stoddard, Privacy Commissioner of Canada	Toronto

Senator N Stott Despoja	Canberra
Suncorp	Sydney
Associate Professor D Svantesson, Faculty of Law, Bond University	Brisbane
Dr S Tan, Clinical Advisor, Western Australian Government Department of Health	Perth
Tasmanian Government Department of Health and Human Services	Hobart
Tasmanian Government Office of the Commissioner for Children	Hobart
Tasmanian Ombudsman and Health Complaints Commissioner	Hobart
Telecommunications Industry Ombudsman	Melbourne/Sydney
Telethon Institute for Child Health Research	Perth
Telstra	Sydney/Melbourne
R Thomas, Information Commissioner, United Kingdom	London
K Thompson, International Center for Law and Religion Studies, Brigham Young University	Sydney
P Timmins, Consulting & Training	Sydney
Toyota Finance Australia Ltd	Sydney
Turner Broadcasting System	Sydney
UNISYS Security Index	Sydney
University of New South Wales, Rural Clinical School	Coffs Harbour
Dr G Urbas, Faculty of Law, Australian National University	Canberra
Veda Advantage	Sydney/Melbourne
Victorian Government Office of the Health Services Commissioner	Melbourne
Vodafone	Melbourne
A Waldo, Chief Privacy Officer, Lenovo	Sydney
N Waters, Pacific Privacy Consulting	Sydney
Dr H Wellington, DLA Phillips Fox	Melbourne

H Wells, School of Social Sciences, Bond University	Brisbane
Western Australian Government Department of Health	Perth
Western Australian Government Office of Children and Youth	Perth
Western Australian Government Office of the Information Commissioner	Perth
Westpac	Sydney
Dr N Witzleb, Faculty of Law, University of Western Australia	Perth
Youth Action and Policy Association	Sydney
Youth Affairs Council of Victoria	Melbourne
Youth Substance Abuse Service	Melbourne

Appendix 3. List of Selected Abbreviations

The entities listed below are Australian entities unless otherwise stated.

2000 House of Representatives Committee inquiry	Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000)
2000 Senate Committee inquiry	Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000)
AAT	Administrative Appeals Tribunal
ABA	Australian Bankers' Association
ABC	Australian Broadcasting Corporation
ABCI	Australian Bureau of Criminal Intelligence
ABN	Australian Business Number
ABS	Australian Bureau of Statistics
ACA	Australian Communications Authority
ACC	Australian Crime Commission
ACC Act	*Australian Crime Commission Act 2002* (Cth)
ACCC	Australian Competition and Consumer Commission
ACCI	Australian Chamber of Commerce and Industry
ACIF	Australian Communications Industry Forum
ACLEI	Australian Commission for Law Enforcement Integrity
ACMA	Australian Communications and Media Authority

ACSI 33	Australian Government Defence Signals Directorate, *Australian Government Information Technology Security Manual* (2007)
ACSQHC	Australian Commission on Safety and Quality in Health Care
ACT	Australian Capital Territory
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977* (Cth)
ADMA	Australian Direct Marketing Association
ADR	Alternative Dispute Resolution
AEC	Australian Electoral Commission
AEEMA	Australian Electrical and Electronic Manufacturers' Association
AFC	Australian Finance Conference
AFP	Australian Federal Police
AFPC	Australian Fair Pay Commission
AGAC	Australian Guardianship and Administration Committee
AGD	Australian Government Attorney-General's Department
AGIMO	Australian Government Information Management Office
AHEC	Australian Health Ethics Committee
AHIA	Australian Health Insurance Association
AHMAC	Australian Health Ministers' Advisory Council
AIATSIS	Australian Institute of Aboriginal and Torres Strait Islander Studies
AIC	Australian intelligence community
AIG	Australian Industry Group
AIHW	Australian Institute of Health and Welfare
AIPD	Australian Institute of Private Detectives

AIRC	Australian Industrial Relations Commission
AJAC	Aboriginal Justice Advisory Council
ALGA	Australian Local Government Association
ALP	Australian Labor Party
ALRC	Australian Law Reform Commission
ALRC 11	Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979)
ALRC 22	Australian Law Reform Commission, *Privacy*, ALRC 22 (1983)
ALRC 77	Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995)
ALRC 85	Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998)
ALRC 95	Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002)
ALRC 96	Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003)
ALRC 98	Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004)
ALRC 102	Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005)
ALRC 102	Australian Law Reform Commission, *Same Crime, Same Time*, ALRC 103 (2006)
ALRC 104	Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*,, ALRC 104 (2006)
AMA	Australian Medical Association

AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
AML/CTF Rules	*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)*
ANAO	Australian National Audit Office
ANF	Australian Nursing Federation
ANZDATA	Australian and New Zealand Dialysis and Transplant Registry
APC	Australian Press Council
APEC	Asia-Pacific Economic Cooperation
APF	Australian Privacy Foundation
APP Charter	Asia-Pacific Privacy Charter
APPA	Asia Pacific Privacy Authorities
APRA	Australian Prudential Regulation Authority
ARC	Administrative Review Council
ARCA	Australasian Retail Credit Association
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
ASIS	Australian Secret Intelligence Service
Assignees Determination	Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006
ASSPA	Aboriginal Sacred Sites Protection Authority
ASTRA	Australian Subscription Television and Radio Association
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
AUSTRAC CEO	Chief Executive Officer of AUSTRAC

Austrade	Australian Trade Commission
AVCC	Australian Vice-Chancellors' Committee
Beijing Rules	*United Nations Standard Minimum Rules for the Administration of Juvenile Justice 1985*
BFSO	Banking and Financial Services Ombudsman
Bio21: MMIM	Bio21: Molecular Medicine Informatics Model
Blunn Report	A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department
CBPRs	cross-border privacy rules
CCLC	Consumer Credit Legal Centre (NSW)
CCTV	Closed Circuit Television
CDE	Census Data Enhancement
CDPP	Commonwealth Director of Public Prosecutions
CFA	Consumers' Federation of Australia
CIPPIC	Canadian Internet Policy and Public Interest Clinic
Classes of Credit Provider Determination	Privacy Commissioner, *Credit Provider Determination No. 2006–4 (Classes of Credit Providers)*, 21 August 2006
CLI	calling line identification
CND	calling number display
COAG	Council of Australian Governments
Code Guidelines	Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001)
Code of Conduct	Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991)
Common Criteria	Common Criteria for Information Technology Security Evaluation

COPPA	*Children's Online Privacy Protection Act 1998* (US)
COSBOA	Council of Small Business of Australia
Council of Europe Convention	Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981)
CRAA	Credit Reference Association of Australia
CRN	Customer Reference Number
CROC	*United Nations Convention on the Rights of the Child 1989*
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSMAC	Community Services Ministers' Advisory Council
CVS	Certificate Validation Service
DBCDE	Australian Government Department of Broadband, Communications and Digital Economy
DCITA	Australian Government Department of Communications, Information Technology and the Arts
DEWR	Australian Government Department of Employment and Workplace Relations
DFAT	Australian Government Department of Foreign Affairs and Trade
DIGO	Australian Government Defence Imagery and Geospatial Organisation
DIO	Australian Government Defence Intelligence Organisation
DLU	Data Linkage Unit
DOHA	Australian Government Department of Health and Ageing
DP 72	Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007)
DPS	Parliament of Australia Department of Parliamentary Services

DRM	Digital Rights Management
DSD	Australian Government Defence Signals Directorate
DVS	National Document Verification Service
ECHR	European Convention on Human Rights
EDR	external dispute resolution
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point of Sale
ENUM	Electronic Number Mapping
EU	European Union
EU Directive	European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995)
FaCSIA	Australian Government Department of Families, Community Services and Indigenous Affairs
FCLC	Federation of Community Legal Centres
FCRA	*Fair Credit Reporting Act 1970* (US)
Flood Report	P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004)
FOI	freedom of information
FOI Act	*Freedom of Information Act 1982* (Cth)
FTC	United States Federal Trade Commission
GBE	government business enterprise
GPS	global positioning system
GTMC	Gene Technology Ministerial Council
HIPA Act	*Health Insurance Portability and Accountability Act 1996* (US)

HPP	Health Privacy Principle
HQCC	Health Quality and Complaints Commission
HREC	Human Research Ethics Committee
HREOC	Human Rights and Equal Opportunity Commission
HTTP	hypertext transfer protocol
HWT	Herald and Weekly Times Pty Ltd
ICAC	Independent Commission Against Corruption
ICAO	International Civil Aviation Organisation
ICCPR	*International Covenant on Civil and Political Rights 1966*
ICO	United Kingdom Information Commissioner's Office
IFSA	Investment and Financial Services Association
IGC	Inter-Governmental Committee on the Australian Crime Commission
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986* (Cth)
IHI	Individual Healthcare Identifier
IIA	Internet Industry Association
IP	Internet Protocol
IP 31	Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006)
IP 32	Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006)
IPART	NSW Independent Pricing and Regulatory Tribunal
IPND	Integrated Public Number Database
IPND Act	*Telecommunications Amendment (Integrated Public Number Database) Act 2006* (Cth)

IPP	Information Privacy Principle
ISCA	Independent Schools Council of Australia
ISP	internet service provider
ITSA	Insolvency and Trustee Service Australia
MasterCard/ACIL Tasman Report	ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004)
MEAA	Media, Entertainment and Arts Alliance
MCCA	Ministerial Council on Consumer Affairs
MCEETYA	Ministerial Council on Education, Employment, Training and Youth Affairs
MOU	memorandum of understanding
MRT	Migration Review Tribunal
MRTD	Machine Readable Travel Documents
NADRAC	National Alternative Dispute Resolution Advisory Council
NAIDWG	National Association for Information Destruction, Australian Members and Stakeholders Working Group
National Archives	National Archives of Australia
National Statement	National Health and Medical Research Council and Australian Vice Chancellor's Committee, *National Statement on Ethical Conduct in Human Research*
NCA	National Crime Authority
NCEC	National Catholic Education Commission
NCRIS	National Collaborative Research Infrastructure Strategy
NCYLC	National Children's and Youth Law Centre
NEAF	National Ethics Application Form
NEHTA	National E-Health Transition Authority

NGN	next generation networks
NHMRC	National Health and Medical Research Council
NHMRC Act	*National Health and Medical Research Council Act 1992* (Cth)
NHPP	National Health Privacy Principle
NNTT	National Native Title Tribunal
NPII	National Personal Insolvency Index
NPP	National Privacy Principle
NRS	National Relay Service
NSWLRC	New South Wales Law Reform Commission
NSWLRC CP 1	New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007)
NTC	National Transport Council
NZ Code	*Credit Reporting Privacy Code 2004* (NZ)
NZLC	New Zealand Law Commission
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines	Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)
OECD Security Guidelines	Organisation for Economic Co-operation and Development *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002)
OH & S	Occupational Health and Safety
ONA	Australian Government Office of National Assessments
OPC	Office of the Privacy Commissioner
OPC Review	Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act 1988* (Cth)
OPPC	Obesity Prevention Policy Coalition

OSB	Australian Government Office of Small Business
OVPC	Office of the Victorian Privacy Commissioner
P3P	Platform for Privacy Preferences
PC	personal computer
PCI	Payment Card Industry
PDA	personal digital assistant
PETs	privacy–enhancing technologies
PIA	Privacy Impact Assessment
PIA Guide	Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006)
PIAC	Public Interest Advocacy Centre
PID	Public Interest Determination
PIM	public interest monitor
PIPED Act	*Personal Information Protection and Electronic Documents Act 2000* (Canada)
PIPP	Personal Information Protection Principle
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PPA	Privacy Performance Assessment
PPP	Public Private Partnership
PPS	Payment Performance System
PRIME	Privacy Identity Management for Europe
Privacy Act	*Privacy Act 1988* (Cth)
Privacy NSW	Office of the NSW Privacy Commissioner
PSIS	Prescription Shopping Information Service

PSM 2005	Australian Government Attorney-General's Department, *Protective Security Manual* (2005)
PSTN	Public Switched Telephone Network
Regulatory Taskforce	Taskforce on Reducing Regulatory Burdens on Business
REIA	Real Estate Institute of Australia
RFID	radio frequency identification
RIS	regulatory impact statement
RRT	Refugee Review Tribunal
RTD	residential tenancy database
SALRC	South African Law Reform Commission
SBS	Special Broadcasting Service
SCAG	Standing Committee of Attorneys-General
SCNS	Secretaries Committee on National Security
Section 95 Guidelines	Guidelines under s 95 of the *Privacy Act 1988* (Cth)
Section 95A Guidelines	Guidelines approved under s 95A of the *Privacy Act 1988* (Cth)
SEHR	Shared Electronic Health Record
Senate Committee privacy inquiry	Parliament of Australia—Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Cth)
SIM	Subscriber Identity Module
SLCD	Statistical Longitudinal Census Dataset
SMS	short message services
SSAT	Social Security Appeals Tribunal
State Records	State Records of South Australia
TFN	Tax File Number

TFN Guidelines	Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992)
TIO	Telecommunications Industry Ombudsman
TPA	*Trade Practices Act 1974* (Cth)
TPID	Temporary Public Interest Determination
UCCCMC	Uniform Consumer Credit Code Management Committee
UHI	Unique Healthcare Identifier
UK	United Kingdom
UN	United Nations
UPP	Unified Privacy Principle
URL	Uniform Resource Locater
US Interagency Guidance	United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005)
US Patriot Act	*Uniting and Strengthening America by Providing Appropriate Tools to Interact and Obstruct Terrorism Act 2001* (US)
VACC	Victorian Automobile Chamber of Commerce
VCEC	Victorian Competition and Efficiency Commission
Victorian Review	2006 Victorian Consumer Credit Review
VLRC	Victorian Law Reform Commission
VoIP	Voice over Internet Protocol
VSCL	Victorian Society for Computers and the Law
Wallis report	Financial System Inquiry Committee, *Financial System Inquiry Final Report* (1997)
Web	World Wide Web

YACVic	Youth Affairs Council of Victoria
YMA	Young Media Australia

Appendix 4. Cost Estimate by Applied Economics

Contents

Summary

Most businesses with a turnover of $3 million or less are currently exempt from complying with the *Privacy Act*. The Office of Small Business (OSB, *Costing into the Review of the Privacy Act*, October 2007) estimated that requiring small businesses to comply with the Privacy Act would cost $3.2 billion in year one.

OSB estimated that 1,805,000 small businesses would be affected at an average weighted cost of $1,765 per business. This included an estimated $842 in start up costs and $924 in ongoing annual costs.

This paper reviews these estimates and finds that OSB overestimated the number of businesses that will be affected by an extension of the *Privacy Act* and, more especially, the average compliance cost per firm. Our analysis suggests that about

1,685,000 businesses will be affected at a weighted average cost per business of $526 in the first year. The estimated total compliance in the first year would be $0.9 billion.

These costs can be broken down into one-off costs ($225 per firm for a total of $380 million) and ongoing annual costs ($301 per firm for a total of $508 million).

The estimates in this paper are only indicative, but nevertheless they are believed to be a much more appropriate order of magnitude cost than the OSB estimates.

Background

Establishing the number of small businesses affected by the proposed change is complicated because the Australian Bureau of Statistics (ABS) publishes data on the number of businesses with turnover of less than $2 million but not on the number with a turnover of between $2 million and $3 million. Furthermore, not all businesses with a turnover of $3 million or less are currently exempt from the Act. A further difficulty in determining the number of businesses affected is that an unknown number do not hold any personal information about staff or customers/clients.

The second stage of the OSB costing process was to determine the steps required to comply with the *Privacy Act* (eleven in all according to OSB) and the cost of each of those steps. The costs ranged from $52 for familiarisation with privacy policy to $499 for promulgating privacy policy.

OSB appears to assume that none of the businesses that would be affected by an extension of the Act currently meet any of the requirements for compliance with the Act. For example, none of the businesses owns a filing cabinet or a paper shredder or has a plan for safeguarding information.

It may also be noted that the breakdown of costs into one-off and ongoing assumes that firms have an ongoing life. The turnover of firms in the small business sector is quite large so that many costs will be annual. In 2006–07, for example, the ABS recorded entries of 330,000 firms with fewer than 20 employees and exits of 280,800 firms of that size.[1]

Number of businesses affected

ABS data on small businesses are hard to reconcile. On the one hand, ABS [2] estimates that there were 1,839,012 firms with turnover of less than $2 million in June 2006. On the other hand ABS[3] estimates that there were 1.88 million firms with fewer than 20 employees also in June 2006. The difference is remarkably small.

---

1 ABS 8165.0, *Counts of Australian Businesses, Including Entries and Exits*, June 2003 to June 2007.
2 Ibid.
3 Ibid. The publication shows that in June 2006 there were 1,156,326 non-employing firms; 494,196 firms with 1–4 employees; and 227,373 firms with 5–19 employees, a total of 1,877,895 firms.

The OSB seems to have used the latter estimate as a proxy for the number of firms with turnover of $3 million or less (although the actual basis for their assumption on numbers is not clear). However, this number would seem to be an overestimate.

A firm with a turnover of $3 million and 19 employees would have turnover of $158,000 per employee. In 2005-06, small businesses (by the ABS definition) in the education and personal and other services industries had turnover per employee of $67,000 and $93,000 respectively.[4] In the accommodation, cafes and restaurants industry turnover per employee was $118,000. By making allowance for statistical discrepancy, most cultural and recreational services where turnover per employee was $161,000 could be smaller firms.

However, in several industries average turnover per employee for smaller firms was well over $158,000 per person. In manufacturing and construction it was $206,000 and $316,000 respectively. In wholesale trade it was $661,000, in transport and storage $329,000 and in property and business services $235,000.

Another ABS publication[5] provides turnover per employee data for firms in the retail industry with fewer than 20 employees. The average turnover per employee for all types of retailing in 2005–06 was over $228,000. Firms with as few as 14 employees would have a turnover over $3 million.

The OSB starting point of 1.88 million small businesses would seem therefore to be an overestimate. On the other hand, as noted ABS also estimates that there were 1.84 million businesses with a turnover of under $2.0 million. For the purpose of this exercise we start by assuming that there are 1.86 million businesses with an annual turnover of $3.0 million or less.

Adjustment for businesses not affected

The OSB then deducts businesses which would not be affected by an extension of the *Privacy Act*. Various small businesses are not exempt from the *Privacy Act* at present. These are mainly businesses that hold health information on individuals but some other types of small business that trade in personal information such as recruitment firms are also covered. Under ss 6D and 6E of the *Privacy Act*, firms not exempt include small businesses that:

- disclose personal information about another individual to third parties for a benefit, service or advantage (unless with the consent of the individual or in accordance with legislation);

4 ABS 8155.0, *Australian Industry 2005–06*.
5 ABS 8622.0, *Retail and Wholesale Industries 2005–06*.

- collect personal information about another individual from third parties by providing a benefit, service or advantage (unless with the consent of the individual or in accordance with legislation);

- provide a health service to another individual and hold any health information except in an employee record;

- are contracted to provide a service to the Commonwealth; or

- are prescribed by regulation as being covered by the legislation.

The OSB subtracted 75,000 firms to account for non-exempt businesses in the health sector. This does not account for the other non-exempt businesses already covered by the Act.

Also many businesses will not be affected because they hold no information covered by the Act. These include non-employing businesses that provide goods and services only to the business sector and/or whose transactions with the household sector are cash transactions.

Examples of businesses which provide goods and/or services to the business sector include consultants, business trades people, most owner/operators of trucks. Businesses that deal in cash with the household sector include butchers, greengrocers, corner shops or convenience stores, and some tradesmen.

In June 2006 there were more than 1.15 million non-employing businesses.[6] Assuming all of them had turnover of $3 million or less, they represent almost 62 per cent of the estimated 1.86 million businesses in that category.

For this exercise we assume that a further 100,000 businesses (in addition to the 75,000 health care businesses) would not be affected by an extension of the *Privacy Act* either because they are already affected by the Act or because the Act would have no application to them.

Subtracting 175,000 from the adjusted starting point figure of 1.86 million small businesses leaves an estimated 1.685 million businesses affected by an extension of the *Privacy Act*.

6 See ABS 8165.0, *Counts of Australian Businesses, Including Entries and Exits*, June 2003 to June 2007.

Assumptions of the costing

Accepting the OSB's 11 steps to comply with the Privacy Act, the estimated costs can be questioned on two grounds.

1. Has the OSB described the only way to take each of these steps or is there an alternative way that could cost less?

2. Might some firms already have taken some of these steps before they were required to do so?

Familiarisation with privacy legislation

The procedure outlined in the OSB document—spending two hours studying educational booklets issued by the Office of the Privacy Commissioner—seems sensible, possibly even a minimum requirement. However, about 1 million of the affected businesses are non-employing and many of these will have personal data on fewer than half a dozen clients/customers. Some other businesses—a butcher, greengrocer or hairdresser—with two or three employees will have no data on customers/clients.

Furthermore, many businesses that have information on employees or customers will already be taking steps to keep that information confidential. That is normal commercial practice.

People in the above categories are unlikely to spend two hours perusing official booklets. They are more likely to get their information on the *Privacy Act* from newspaper reports, articles in magazines (including trade magazines), from conversations with other business people and as free advice from their accountant.[7]

Much of this gathering of information is effectively costless. The business people were going to read the newspaper and magazine anyway or converse with other business people on matters of mutual interest. Or they would learn about the *Privacy Act* from their accountant in the routine course of business.

Assume, however, that this informal approach costs[8] one hour and is used by 80 per cent of small businesses whereas the formal approach costing two hours is used by the other 20 per cent. The average cost of familiarisation is the $(0.8 \times \$26) + (0.2 \times \$52)$ which equals $31.20 per business or a total of $52.6 million.

---

7 These are the methods used by most people to acquaint themselves with the regulations concerning self managed super funds.

8 The hourly costs used in this paper are those used by OSB, i.e. $26/hour internal and $100/hour outsourced.

Conduct a privacy audit

Most small businesses have personal information about fewer than half a dozen people. Many of these firms, out of self interest, will already have taken measures to safeguard that information. They will not need two hours to conduct a privacy audit. Here we assume that 50 per cent of businesses see no need for a formal privacy audit; 30 per cent spend one hour conducting an in-house audit; and 20 per cent outsource a two hour audit at $100 per hour. The average cost is thus (0.5 × $0) + (0.3 × $26) + (0.2 × $200) which comes to $47.80 while the total cost for all businesses is $80.5 million.

Develop a privacy plan

"*Small businesses will need to consider how they will implement the privacy provisions that regulate the way they collect, hold, use, keep secure and disclose* ***personal*** *information".*[9] This is true for every business regardless of the *Privacy Act*. Businesses have information that must be kept secure and disclosed when necessary. An extension of the *Privacy Act* does not change that, although it may sometimes increase the amount of information that must be kept secure.

The OSB considers that small business will spend on average three hours in developing a privacy plan if the *Privacy Act* is extended even though "some small businesses may not need to develop a privacy plan".[10] This seems an overestimate.[11]

However, some businesses coming within the ambit of the Act do not have a plan for keeping information secure. Developing a plan should be considered a cost of doing business, but it is accepted here that extending the *Privacy Act* may require 20 per cent of affected businesses to spend three hours in-house developing a privacy plan. The estimated cost is a weighted average of $15.60 per firm or a total of $26.3 million.

Amend business documentation

Many businesses will not amend business documentation. What part of a butcher shop's advertising requires "general information on their small business privacy policy"? How often is a customer required to sign a contract before a barber cuts their hair? A small proportion of small businesses may have to amend some business documentation but most will rely on advice from trade magazines and/or trade organisations. The changes will occur over time, not when an extended *Privacy Act* becomes law.

We assume however that 20 per cent of small businesses will outsource this task to a legal professional. The estimated cost per firm will be 0.20 × $100 = $20 and the total cost will be $33.7 million.

---

9 *Costing the Review of the Privacy Act 1988*, OSB.

10 OSB, *loc sit.*

11 Costs may also be reduced if the Office of the Privacy Commissioner develops and publishes templates for small businesses to follow in preparing privacy policies as proposed by the ALRC.

Train staff

The training policy can apply only to businesses with employees. In June 2006 there were 1,156,000 non-employing businesses in Australia.[12] As this includes some large businesses that would be outside our base figure of 1,685,000 small firms, we subtract the estimated number of non-employing businesses from the OSB estimate of 1,805,000 businesses affected by an extension of the *Privacy Act* to obtain an estimate of 649,000 small businesses with employees. Multiplying the weighted average cost of $89 per business by 1,805,000 provided OSB with an estimated cost of $160.6 million. Using a multiplier of 649,000 businesses, the total cost would be $57.8 million.

Purchase a filing cabinet and paper shredder

OSB assumes that all small businesses would need to purchase a filing cabinet and a paper shredder at a combined cost of $378. This assumes unrealistically that these would be required but not currently possessed.

At a stretch, 20 per cent of small businesses might need to purchase these items. The average cost per business then would be $0.2 \times \$378 = \$76$ and the total cost would be $128.1 million.

Firms that store data on computer files would need security measures, but that is a need they already face. An extension of the *Privacy Act* will not extend that need, but it might give businesses that have not taken proper security measures a greater incentive to do so.

Handle customer complaints/requests

OSB guesses that small businesses may have to deal with an average of one complaint a month (12 a year) at a time of 30 minutes ($13) per complaint and a cost of $156 per year. There appears to be no evidence base for these assumptions.

On the other hand the ALRC has pointed out to us that in 2005–06 the Office of the Privacy Commissioner received only 420 complaints in relation to small businesses. While this is not a direct indicator of the number of complaints that would occur if small businesses were not exempt from the Act, it does suggest that an average of a complaint a month for each small business is a significant overestimate.

On the other hand, whereas the cost of dealing with most complaints would be quite small, some businesses may face high costs in dealing with serious or vexatious complaints.

12 ABS 8165.0, *Counts of Australian Businesses, Including Entries and Exits.*

Allowing for one complaint per business per quarter but a higher average cost of $30 per complaint, the average annual cost would be $120 per business instead of the OSB estimate of $156 per business. Multiplying by 1.685 million businesses, the total cost per year would be $202.2 million.

Secure record keeping

The OSB estimated that secure record keeping would involve 10 minutes a week in record keeping and filing. Using their estimate of 1.805 million businesses, the cost of 10 minutes per week at $26 an hour is $407 million per year (not $414 million as per their paper).

However, in our view for many businesses there would be no incremental work or record keeping over and above what businesses already do. Using the same unit cost and applying this to 50 per cent of our estimate of 1.685 million affected businesses, the total cost would be $189.7 million a year.

Promulgate privacy policy

According to the ABS, 40 per cent of businesses with 5 to 15 employees have a website and so could publish their privacy policy at little if any cost.[13]

However, if the *Privacy Act* is extended some small businesses may need to have available a hard copy document showing how they handle personal information. A few small businesses, for example those that deal with governments or large corporations, may feel the need to have 500 copies of a colour brochure printed at a cost of $499.

Other small businesses that feel a need to disseminate their privacy policy will use their computer to create a document and print out copies as required at a cost in the order of $0.50 per copy and a total cost of $10.

This paper assumes that 5 per cent of firms will be in the first category and 50 per cent of firms in the second. The average cost per firm will be $(0.05 \times \$499) + (0.50 \times \$10) = \$29.95$. The total cost for small businesses will be $50.5 million.

Update/review privacy policy

This note accepts that in the course of a year small businesses will, on average, spend an hour and a half reviewing and updating their privacy policy. Such reviews and updates are likely to result from reading about privacy policy in a newspaper or business magazine or following conversations with other business people.

---

13 ABS, 8129.0, *Business Use of Information Technology, 2005–06*.

Applying the cost per business of $39 per year to 1.685 million affected businesses, the total cost is $65.7 million.

Conclusions

The following table summarises the results of our assumptions and estimates. The estimated weighted average cost per business is $526 and the total cost is $888 million.

These costs can be broken down into one-off costs ($225 per firm for a total of $380 million) and ongoing annual costs ($301 per firm for a total of $508 million).

The estimated cost to small businesses of extending the coverage of the *Privacy Act* is much smaller than the compliance cost estimated by OSB.

Part of the difference reflects the assumption that fewer businesses will be affected by an extension of the *Privacy Act* (1.685 million compared to 1.805 million).

This is because the OSB makes no adjustment for some firms already covered by the Act. In addition, some small firms will not be affected in any significant way by an extension of the Act because they have no information covered by the Act.

Other differences relate to assumptions about the costs to businesses. For example, the OSB assumption that every small business would need to purchase a filing cabinet and paper shredder and have 500 copies of a colour brochure printed is quite unrealistic. Also the assumption about training costs can apply only to businesses that employ people. OSB applied the costing to all of the 1.805 million small businesses. However these are only examples of differences. There were many others as described above.

Summary of cost estimates in this paper

Small business task	Weighted average cost per business ($)	Total cost $m
Familiarisation with legislation	31	53
Conduct privacy audit	48	81
Develop a privacy plan	16	26
Amend business documentation	20	34
Train staff	34	58
Purchase filing cabinet and shredder	76	128
Handle customer complaints	120	202
Record keeping	112	189
Promulgate privacy policy	30	51
Update/review privacy policy	39	66
Total	**526**	**888**

Notes on authors

Dr. Peter Abelson has a Ph.D in economics from the University of London. He is a Director of the economic consultancy, Applied Economics. From 2001 to 2005, Peter held a Personal Chair in Economics at Macquarie University. He currently holds visiting positions at the University of Sydney and the University of New South Wales and is an Adjunct Professor with the Australian and New Zealand School of Government. He also works two days a week as a principal economic advisor to the NSW Treasury. McGraw-Hill is publishing the second edition of Peter's major Australian text "Public Economics: Principles and Practice" in late February 2008.

David Maynard has a Masters degree in economics from the University of Alberta and was a lecturer for nine years at the University of New England. David worked for 20 years as an economist with the NSW Treasury. He now works with Applied Economics.

Appendix 5. Table of Selected Legislation

Only legislation discussed in some detail in the text is listed below. The *Privacy Act 1988* (Cth) is not listed. The *Privacy Act* and other legislation can be located in the text using the full text search facility available on the internet and CD versions of this Report. References are to paragraphs or chapters in this Report.

Australia

Victoria

Queensland

Western Australia

United Nations

United States

Other International

Index