Australian Government

Australian Law Reform Commission

For Your Information

REPORT

Australian Privacy Law and Practice

Volume 2
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 D

The Privacy Principles

Continued

25. Use and Disclosure

Contents

Introduction

25.1 Research conducted in 2001 on behalf of the Office of the Privacy Commissioner (OPC) indicated that Australians were worried about the use of personal information for a purpose other than the original purpose for which it was collected. Of 1,524 people interviewed, 68% stated that this was a concern to them, 41% stated it

was a great concern and 23% recorded little or no concern.[1] Similarly, 37% of complaints to the OPC under the National Privacy Principles (NPPs) in the financial year ending 30 June 2007 related to the use or disclosure of personal information.[2] This represented the largest single category of complaint.

25.2 The Information Privacy Principles (IPPs) and NPPs adopt a prescriptive approach to regulating the use and disclosure of personal information. The use provisions in the IPPs and NPPs, and the disclosure provisions in the NPPs, prohibit the use and disclosure of personal information for a purpose other than the purpose for which the information was collected. This general prohibition is subject to an exhaustive list of exceptions.

25.3 This chapter considers whether the use and disclosure provisions in the IPPs and NPPs should be consolidated into a single use and disclosure principle in the model Unified Privacy Principles (UPPs). It also considers the limited circumstances in which agencies and organisations should be permitted to use and disclose personal information for a purpose other than the original purpose of collection. Finally, the chapter addresses the issue of whether agencies and organisations should be required to record their use and disclosure of personal information for a purpose other than the purpose of collection.

Current coverage by IPPs and NPPs

25.4 IPPs 9 to 11 deal with the use and disclosure of personal information by agencies. IPP 9 provides that personal information may be used only for relevant purposes. IPPs 10 and 11, respectively, impose limitations on the use and disclosure of personal information. For organisations, the rules on the use and disclosure of personal information are set out in a single privacy principle, NPP 2.

25.5 NPP 2 prohibits the use and disclosure by an organisation of personal information for a purpose other than the primary purpose of collection (the secondary purpose) except in specified circumstances. The IPPs do not use the language of 'primary' and 'secondary' purpose. IPP 10 provides that where an agency obtains personal information for a 'particular purpose', it cannot use the information for any 'other purpose' except in specified circumstances. The concepts underlying NPP 2 and IPP 10, therefore, are substantially similar. IPP 11 simply restricts the disclosure of personal information by agencies except in specified circumstances. It does not refer to the particular purpose for which personal information was collected.

---

1 Roy Morgan Research, *Privacy and the Community [prepared for Office of the Federal Privacy Commissioner]* (2001), 25.

2 See Office of the Privacy Commissioner, *Complaints and Enquiries Statistics to End of June 2007* <www.privacy.gov.au/about/complaints/index.html> at 14 May 2008.

25.6 There are some important similarities between the specified circumstances in the IPPs and NPPs that authorise the use and disclosure of personal information. Each of IPP 10, IPP 11 and NPP 2 permit use and disclosure where:

- the individual has consented to the use or disclosure;
- it is required or authorised by or under law; or
- it is necessary to prevent or lessen a serious and imminent threat to the life or health of an individual.

25.7 The IPPs and NPPs cover common ground in another area. Under the IPPs, use or disclosure is permitted where it is reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty or protect the public revenue. Under the NPPs, use or disclosure on these grounds is permissible where an organisation reasonably believes that it is reasonably necessary for certain activities by or on behalf of an enforcement body. The test in the IPPs is, therefore, more objective than that in the NPPs.

25.8 There are, however, important differences between the NPPs and IPPs concerning use and disclosure. These differences are discussed fully below. A key difference is that the NPPs contain a greater number of exceptions to the general prohibition against use and disclosure for a secondary purpose than the IPPs. In particular, NPP 2 permits use or disclosure for a secondary purpose:

- for the safety of an individual, public health and public safety;
- in the preparation for, or conduct of, court or tribunal proceedings;
- for direct marketing for non-sensitive information where specified criteria are met;[3]
- as a necessary part of an organisation's investigation of suspected unlawful activity or for reporting its concerns to the authorities;
- where the organisation reasonably believes that the use or disclosure is reasonably necessary for certain specified functions of an enforcement body, including: the investigation of seriously improper conduct or prescribed conduct; enforcement of laws relating to the confiscation of the proceeds of crime; or preparation for, or conduct of, court or tribunal proceedings;

---

3 Direct marketing is dealt with separately in Ch 26. It is the subject of UPP 6, applicable only to organisations.

- of health information for research or statistics relevant to public health and safety where specified criteria are met;

- by an organisation that provides a health service to an individual of health information about that individual to a person 'responsible' for the individual if certain conditions are met; or

- of genetic information obtained in the course of providing a health service to the individual where specified criteria are met.

25.9 In addition, unlike the IPPs, NPP 2 contains notes that indicate that NPP 2 is not intended to deter organisations from lawfully cooperating with law enforcement agencies and that an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.[4]

25.10 Both the IPPs and NPPs require the use and disclosure of personal information for law enforcement purposes to be recorded.[5]

A single 'Use and Disclosure' principle

25.11 As noted above, the IPPs contain separate 'use' and 'disclosure' principles. In contrast, the NPPs, and the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines), deal with use and disclosure in a single privacy principle.[6]

25.12 In assessing the merits of dealing with use and disclosure in one principle, consideration needs to be given to the meanings of 'use' and 'disclosure'. Section 6(1) of the *Privacy Act 1988* (Cth) provides that:

> ***use***, in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication.

25.13 The *Privacy Act* does not otherwise define 'use', nor does it define the concept of disclosure. Guidance issued by the OPC on the IPPs addresses the meaning of 'use'. It provides that:

> Use is interpreted broadly. It relates to managing personal information with an agency. As a general rule, any accessing by an agency of personal information in its control is a 'use'. This includes:
>
> - searching records for any reason

---

4 See *Privacy Act 1988* (Cth) sch 3, NPP 2, Notes 1–3.

5 Ibid sch 3, NPP 2.2; s 14, IPPs 10.2, 11.2.

6 See Ibid sch 3, NPP 2 and Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 9. The privacy principles contained in the OECD Guidelines are set out in Ch 1.

- using personal information in a record to make a decision
- passing a record from one part of an agency to another part with a different function.[7]

25.14 The OPC's guidance also addresses the meaning of disclosure, and provides examples of disclosures. It states that:

> The Privacy Commissioner interprets disclosure as a release of personal information from the effective control of the agency. An agency may release the personal information:
>
> - automatically, to a person or body that the agency knows has a general authority to access that personal information; or
> - in response to a specific request.[8]

25.15 The OPC's guidance states that an agency's action cannot be both a use and disclosure.[9] This means that an agency has to decide whether to apply the principle relating to use, or that relating to disclosure. The guidance considers the circumstances in which passing personal information outside an agency is a 'use'. It states that the test for categorising an action as a use or disclosure 'is always whether or not the agency maintains control over that personal information'.[10]

Submissions and consultations

25.16 In Issues Paper 31, *Review of Privacy* (IP 31) the ALRC asked whether the IPPs, in addition to the NPPs, should deal with use and disclosure in one privacy principle.[11] In response to IP 31, a majority of stakeholders stated that agencies should be subject to a single privacy principle dealing with use and disclosure. The OPC submitted that a single use and disclosure principle would

> assist in providing a consistent approach for the handling of personal information and may go some way to alleviating the confusion that surrounds the identification of whether certain activities and information handling practices are considered a 'use' or a 'disclosure' and which provisions and principles should apply.[12]

---

7 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), 11–12.

8 Ibid, 12.

9 Ibid, 12.

10 Ibid, 12. The OPC's guidance also addresses the circumstances when an agency maintains control over personal information. See Ibid, 13.

11 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–6.

12 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

25.17 A number of other stakeholders expressed a similar view.[13] The National Health and Medical Research Council (NHMRC) noted that often 'whether an information transaction is a "use" or a "disclosure" is determined by corporate structures rather than by practical differences in information-handling practices'.[14]

25.18 Some private sector stakeholders also favoured a single use and disclosure principle. It was submitted that where a private sector organisation must comply with the IPPs pursuant to a contract it has entered into with a public sector entity, it would be 'useful' for the Act to deal 'consistently with the principles relating to all dealings with personal information, including use and disclosure'.[15]

25.19 Other stakeholders preferred that agencies be subject to separate use and disclosure principles.[16] For example, the Australian Federal Police (AFP) expressed the view that the current structure of the IPPs is working adequately and does not need to be changed.[17] The Department of Human Services submitted that separate principles align better with 'secrecy provisions' in other legislation.[18]

25.20 In Discussion Paper 72, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that agencies and organisations should be subject to a single use and disclosure principle.[19] A majority of stakeholders supported this proposal.[20] Reasons for support included that it would:

---

13 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Confidential, *Submission PR 130*, 17 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; I Turnbull, *Submission PR 82*, 12 January 2007.

14 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

15 National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007. See also National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

16 Australian Federal Police, *Submission PR 186*, 9 February 2007; Confidential, *Submission PR 143*, 24 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; W Caelli, *Submission PR 99*, 15 January 2007.

17 Australian Federal Police, *Submission PR 186*, 9 February 2007.

18 Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

19 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 22–1.

20 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. Another stakeholder stated that it did 'not oppose' the proposal: National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

- reduce significantly the complexity in privacy regulation;[21]
- avoid technical legal arguments, and confusion, about whether an action is a use or disclosure and therefore which principle applies;[22] and
- result in a more workable regime.[23]

25.21 The Cyberspace Law and Policy Centre emphasised that, even with the adoption of a single principle, it is necessary to understand the meaning of the distinct concepts of use and disclosure.[24] The Australian Privacy Foundation expressed the view that the 'Use and Disclosure' principle, the definitions or the Explanatory Memorandum to the amending legislation should:

- confirm that accessing personal information of itself constitutes use; and
- clarify the circumstances in which passing information outside an organisation remains a use, rather than a disclosure.[25]

25.22 The Cyberspace Law and Policy Centre stated that it would be 'unwise' to apply to the private sector the OPC's interpretation of the distinction between a use and disclosure 'without further consideration'. It also submitted that the 'Use and Disclosure' principle, the definitions or the Explanatory Memorandum to the amending legislation should make it clear that

> there can be a disclosure even if the information is not used or acted on by the third party, and that even [if] information [is] already known to the recipient it can be disclosed.[26]

25.23 The Queensland Government stated that it

> has not encountered any specific difficulties with use and disclosure being addressed in different principles, nor does it see any pressing reason why they need to be combined. It is noted, however, that, given the exceptions to each general principle—i.e. use for a secondary purpose—are to be identical, combining the two does allow for a more concise statement of the principles.[27]

---

21 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
22 See, eg, Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.
23 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
24 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
25 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. Another stakeholder expressed a similar view: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
26 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
27 Queensland Government, *Submission PR 490*, 19 December 2007.

25.24 Medicare Australia expressed a preference for the retention of separate principles dealing with use and disclosure because this aligns better with its secrecy provisions. It acknowledged, however, the vast support for the contrary view.[28]

ALRC's view

25.25 The use and disclosure of personal information should be dealt with in one privacy principle, which should apply both to agencies and organisations. This is consistent with the process of consolidating the IPPs and NPPs into a single set of privacy principles, the UPPs.[29]

25.26 Moreover, dealing with use and disclosure in a single principle will reduce the complexity in privacy regulation. It will avoid technical legal arguments about whether an action constitutes a use or disclosure, and therefore reduce confusion about which principle should apply.

25.27 Having the same rules apply to use and disclosure, however, will not conflate the two concepts. It will continue to be necessary for agencies and organisations to understand their meaning. As stated in the OPC's guidance, a key factor in distinguishing between use and disclosure is whether the entity maintains control over the personal information. It would be inconsistent with the adoption of high-level principles to introduce detailed and prescriptive rules about each of the circumstances in which particular actions will constitute use or disclosure.

25.28 Further, it is unnecessary for the *Privacy Act* to make it clear that accessing personal information amounts to use. The OPC's guidance on this issue states expressly that 'as a general rule, any accessing by an agency of personal information in its control is a "use"'. Similarly, it is unnecessary to clarify legislatively that personal information can be disclosed even if the information is not used or acted on, or is known, by the recipient, as suggested by one stakeholder. A common sense approach to interpreting the act of disclosure focuses on the act done by the disclosing party—that is, the act of releasing personal information from its control. The state of mind or intentions of the recipient cannot negate an act of disclosure, although they may limit the privacy consequences that might ensue.

Recommendation 25–1 The model Unified Privacy Principles should contain a principle called 'Use and Disclosure' that sets out the requirements on agencies and organisations in respect of the use and disclosure of personal information for a purpose other than the primary purpose of collection.

28 Medicare Australia, *Submission PR 534*, 21 December 2007.
29 See Ch 18, Rec 18–2.

Circumstances in which use and disclosure is permitted

25.29 Compared to some other principles in the *Privacy Act*, the principles relating to use and disclosure in each of the IPPs and NPPs adopt a prescriptive approach. They do not contain an overriding qualifier, such as permitting use or disclosure where it is 'reasonable' in the circumstances.[30]

25.30 The use and disclosure of personal information for the primary purpose for which it was collected is permissible. Other use and disclosure is prohibited unless it falls within the ambit of a specific legislative exception. The exceptions authorise, but do not require, a use or disclosure to be made. A note to NPP 2 provides that the principle

> does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.[31]

25.31 The discussion below considers the circumstances that may comprise exceptions to a general prohibition against the use or disclosure of personal information for a purpose other than that for which it was collected.

Related or directly related secondary purpose

25.32 It is possible for agencies and organisations to use personal information, and for organisations to disclose personal information, where the purpose for which the information is to be used or disclosed (the secondary purpose) has the requisite connection with the primary purpose of collection.

25.33 NPP 2.1(a) allows the use or disclosure of personal information for a secondary purpose if the:

- secondary purpose is related to the primary purpose of collection,[32] or, if the information is 'sensitive information', the secondary purpose is *directly* related to the primary purpose; and

- individual would reasonably expect the organisation to use the information for the secondary purpose.

---

30 Compare the approach taken in NPP 1.4, for example, which requires an organisation to collect personal information about an individual only from that individual, if it is reasonable and practicable to do so.

31 *Privacy Act 1988* (Cth) sch 3, NPP 2.1, Note 2.

32 The Explanatory Memorandum stated that 'to be "related", the secondary purpose must be something that arises in the context of the primary purpose': Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [341].

25.34 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector Bill) 2000 justified the imposition of a stricter test in respect of the use and disclosure of sensitive information under the NPPs. It stated that:

> The sensitivities associated with the use or disclosure of sensitive information mean that a stronger connection should be demonstrated between the primary purpose for collection and the secondary purpose.[33]

25.35 In contrast, IPP 10.1(e) imposes the stricter test of having to establish, in each case, a direct relation between the purpose of collection and the proposed secondary use of personal information.[34] IPP 10.1(e) does not impose, however, the additional 'reasonable expectation' test that is provided in NPP 2.1(a).

25.36 IPP 11 does not contain an equivalent provision to NPP 2 1(a). It allows for disclosure, however, where the individual concerned is reasonably likely to have been aware, or made aware, that information of that kind is usually passed to the entity to which the disclosure is to be made. Under this exception, there is no requirement for an agency to establish any connection between the purpose of collection and the disclosure.

Submissions and consultations

Connection between primary and secondary purpose: direct or indirect?

25.37 In response to IP 31, a number of stakeholders expressed the view that the use and disclosure of personal information by agencies and organisations for a secondary purpose should be allowed only where that purpose is directly related to the primary purpose of collection.[35] Other stakeholders opposed a requirement that there be a 'direct' relationship between the purpose of collection and the secondary purpose for which personal information is to be used or disclosed.[36] For example, the Commonwealth Scientific and Industrial Research Organisation (CSIRO) expressed concern that such an amendment 'would introduce further restrictions on public health research'.[37]

---

33 Ibid, [342].

34 *Privacy and Personal Information Protection Act 1998* (NSW) s 17(b) also imposes a 'direct relationship' test in the context of use of personal information by agencies.

35 See, eg, 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; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Insolvency and Trustee Service Australia, *Submission PR 123*, 15 January 2007.

36 CSIRO, *Submission PR 176*, 6 February 2007; ANZ, *Submission PR 173*, 6 February 2007.

37 CSIRO, *Submission PR 176*, 6 February 2007. See also Veda Advantage, *Submission PR 163*, 31 January 2007.

Reasonable expectation of use or disclosure

25.38 In response to IP 31, a number of stakeholders supported extending to agencies the requirement, already applicable to organisations, that the individual concerned would reasonably expect the agency to use or disclose the personal information for the secondary purpose in question.[38]

25.39 For example, the OPC stated that the reasonable expectation requirement is meant to be understood in a common sense way and is not overly onerous. It said that if an entity is unsure of the reasonable expectations of an individual in particular circumstances, it could seek the individual's consent. It also expressed the view that IPP 10 already includes the concept of reasonable expectation.[39] On the other hand, there was some concern that a 'reasonable expectation' requirement is 'too vague and open to severe abuse'—particularly, by those engaging in data-mining.[40]

25.40 Some stakeholders opposed the 'reasonable expectations' test being applied to agencies, stating that the current provisions are adequate.[41] For example, the Department of Families, Community Services and Indigenous Affairs (FaCSIA) submitted that such a requirement would restrict how an agency uses personal information and 'could ultimately limit the extent to which an agency could assist individuals'. It stated that:

> Where information about an individual is collected for the purposes of providing a particular programme, FaCSIA considers it important to retain the discretion to use such information for other reasonable purposes, such as to identify and notify the individual of another programme which the individual may benefit from.[42]

---

38 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 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; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

39 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

40 W Caelli, *Submission PR 99,* 15 January 2007.

41 Confidential, *Submission PR 165,* 1 February 2007; AXA, *Submission PR 119,* 15 January 2007.

42 Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

Response to Discussion Paper proposal

25.41 In DP 72, the ALRC proposed that the test in NPP 2.1(a) should apply to agencies and organisations. That is, the 'Use and Disclosure' principle should allow an agency or organisation to use or disclose personal information for a purpose other than the primary purpose of collection if the:

- secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the purpose of collection; and

- individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.[43]

25.42 Most stakeholders supported this proposal.[44] Reasons for support included that the suggested approach:

- would provide more flexibility in the use of personal information than is currently available to agencies under IPP 10;[45]

- maintains the necessary level of privacy protection;[46]

- would introduce an appropriate level of privacy protection concerning disclosures by agencies, given that agencies can currently disclose personal information for *any* unrelated purpose provided that the individual concerned is informed;[47]

---

43 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 22–2.

44 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 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; Queensland Government, *Submission PR 490*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. Another stakeholder stated that it did 'not oppose' the proposal: National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

45 Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.

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

47 Ibid.

- has generally proven effective in balancing privacy and operational requirements in how organisations handle personal information;[48] and

- is a suitable mechanism also for dealing, in an effective manner, with the use and disclosure of personal information by agencies.[49]

25.43 Privacy NSW supported the proposal but suggested that the wording of the principle be simplified along the following lines:

> Where personal information is collected for a purpose it may be used/disclosed for a different purpose, only if that second purpose is somehow related to the original purpose, and only if the individual would reasonably expect the organisation or agency to do so.[50]

25.44 Centrelink noted that its customers generally expect it to use their personal information 'in order to assess their eligibility to the various payments they may claim or transfer between'. It stated:

> It is important, therefore, to ensure that the interpretation of … what an individual would reasonably expect … meets the expectations and needs of individuals and allows for efficient business flows.[51]

25.45 The NHMRC supported the proposal, but expressed concerns about its implementation in the context of health care, and health and medical research. It said:

> Specifically, there is ongoing confusion about whether an individual's consent needs to be obtained when a health care provider organisation seeks or is asked to disclose health information to another health care provider organisation for the purposes of ongoing patient care, or whether such disclosure falls within the 'reasonable expectation' provisions.[52]

25.46 A small number of stakeholders opposed the proposal[53] or parts of the proposal.[54] The Public Interest Advocacy Centre (PIAC) opposed the proposed test concerning the relationship between the primary and secondary purposes. It stated that:

> The requirement of a direct relationship between the secondary and primary purposes should apply for both sensitive and non-sensitive personal information. PIAC sees no

---

48 Ibid**.** Optus expressed a similar view. It stated that the inclusion of a 'reasonable expectation' provision has provided 'useful guidance in many instances during day-to-day operations and decision-making processes within [its] organisation': Optus, *Submission PR 532,* 21 December 2007.

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

50 Privacy NSW, *Submission PR 468,* 14 December 2007. Another stakeholder expressed the view that the terms 'primary' and 'secondary' purpose are outdated: Smartnet, *Submission PR 457,* 11 December 2007.

51 Australian Government Centrelink, *Submission PR 555,* 21 December 2007.

52 National Health and Medical Research Council, *Submission PR 397,* 7 December 2007. The ALRC's view on these concerns is set out in Ch 63, in the discussion on use and disclosure of health information for primary and secondary purposes.

53 Australian Taxation Office, *Submission PR 515,* 21 December 2007.

54 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

> reason for adopting the less stringent requirement of 'related' when research indicates that most Australians have a high level of concern about use of their personal information for a purpose other than its original purpose.[55]

25.47 The Australian Taxation Office (ATO) stated that, 'the proposal, if enacted, would represent a significant and problematic narrowing of the use principle for agencies'. It expressed concern that the introduction of a reasonable expectations test would make the use principle difficult to apply.

> A principle which requires hypothesising what a particular individual would expect, even what they would reasonably expect is, while better than trying to imagine what that person actually expected, still a difficult test. The individual's view of what was reasonable for them is likely to differ from that of the agency. Knowledge of the agency's functions and range of potential uses of information will vary.
>
> The Tax Office does of course inform individuals of anticipated and usual uses of personal information collected about themselves … But uses will arise which we suggest would be reasonably viewed as related, if not directly related, to the original purpose for which the information was collected, even though the individual concerned (perhaps not even the agency itself) could have anticipated them. On the reading of this proposal as it currently stands, we could effectively be prevented from using this information for legitimate and reasonable purposes.[56]

25.48 Finally, some stakeholders supported the OPC developing guidance on the application of the proposed exception.[57] For example, Medicare Australia stated that such guidance would be needed 'to assist agencies [to] manage any differences of opinion with their customers, given the requirement to make an assessment of what the individual would "reasonably expect"'.[58]

ALRC's view

Scope of exception

25.49 The exceptions relating to use and disclosure of personal information as they apply to agencies and organisations should be consolidated. The particular exception in the NPPs allowing use or disclosure for a secondary purpose where there is a requisite connection with the primary purpose of collection, and within the reasonable expectations of the individual, also should apply to agencies. As noted above, the exception appears to be operating effectively in the private sector. Extending its application to the public sector is consistent with the general approach of using the NPPs as templates in drafting the UPPs.[59]

---

55 Ibid.
56 Australian Taxation Office, *Submission PR 515*, 21 December 2007.
57 Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007. See also Centre for Law and Genetics, *Submission PR 497*, 20 December 2007.
58 Medicare Australia, *Submission PR 534*, 21 December 2007.
59 See Ch18.

25.50 Moreover, adopting a two-pronged test which focuses both on the relationship between the primary and secondary purposes, and the reasonable expectations of an individual, achieves an appropriate level of privacy protection. First, it provides additional protection concerning the use and disclosure of sensitive information, commensurate with the risks associated with the improper use and disclosure of such information. It is not necessary or desirable in respect of non-sensitive information to require a direct relationship between the primary and secondary purposes. The imposition of a stricter test of 'direct relation' could be quite onerous for organisations, effectively requiring them to seek consent whenever they wish to use or disclose an individual's personal information for a purpose that is related to the primary purpose of collection, but not directly so. This scenario is likely to arise frequently where an individual is a customer of a large organisation that handles the individual's personal information for multiple products or services. There also is a concern that a direct relationship test may hamper legitimate health and other research.[60]

25.51 Further, to the extent that the current principle regulating use of personal information by agencies will be loosened—in that a direct relationship between the primary and secondary purposes no longer will be required for non-sensitive information—it will be balanced by the additional protection offered by the reasonable expectations test. The imposition of a reasonable expectations test is unlikely to be particularly onerous. It does not require an agency or organisation to consult the individual on each proposed secondary use or disclosure. It is arguable, as the OPC submitted, that such a requirement already is implied in IPP 10.1(e). The fact that a primary purpose is related to a secondary purpose increases the likelihood that an individual would reasonably expect his or her personal information to be used or disclosed for that secondary purpose.

25.52 The recommended approach also is preferable to the current principle governing disclosure of personal information by agencies. It is unsatisfactory that an agency can disclose personal information merely on the basis that the individual concerned is reasonably likely to have been aware, or made aware, that information of that kind is usually disclosed to a particular entity. The existing approach, for example, may disadvantage an individual, who is told after the collection of his or her personal information that it will be disclosed to a particular entity even though the proposed disclosure appears to have minimal connection with the reason the information was collected.

---

60 See Part H for a discussion on use and disclosure of personal information for secondary purposes in the health and research contexts; and Part J for a discussion of use and disclosure in the telecommunications context.

Drafting

25.53 The 'Use and Disclosure' principle, drafted by the ALRC for inclusion in the model UPPs is intended only as a guide or template. Stakeholder concerns about the drafting of this particular exception—for example, those voiced by Privacy NSW—will be best addressed by the Office of Parliamentary Counsel.[61]

Guidance

25.54 The ALRC anticipates that the OPC will develop and publish general guidance to assist agencies and organisations to comply with the 'Use and Disclosure' principle. This will be beneficial, particularly in assisting agencies in their transition to adopting the recommended provisions. The ALRC notes stakeholder support for such an approach. In the absence of a need to nominate any particular area upon which such guidance should focus, it is unnecessary for the ALRC to make a specific recommendation in this regard.

Recommendation 25–2 The 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose other than the primary purpose of collection (the secondary purpose), if the:

(a) secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(b) individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.

Consent

25.55 The IPPs and NPPs each allow personal information to be used and disclosed if an individual has consented to that use or disclosure.

25.56 In DP 72, the ALRC included in its draft 'Use and Disclosure' principle, an exception to the general prohibition on secondary use and disclosure of personal information, in circumstances where an individual has consented to the use and disclosure.[62]. Stakeholders did not express opposition to the retention of this exception. The Cyberspace Law and Policy Centre supported it expressly.[63]

---

61 See Ch 18.
62 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), UPP 5.1(b).
63 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

ALRC's view

25.57 The 'Use and Disclosure' principle should contain an exception authorising the use or disclosure of personal information by agencies and organisations where an individual has consented to that use or disclosure.[64]

Emergencies, disasters and threats to life, health or safety

25.58 The IPPs and NPPs each allow personal information to be used and disclosed if it is necessary to lessen or prevent a serious and imminent threat to an individual's life or health.[65] The NPPs also allow secondary use and disclosure if it is necessary to lessen or prevent a:

- serious and imminent threat to an individual's safety; or
- serious threat to public health or public safety.[66]

25.59 The NPPs, therefore, do not require a threat to public health or public safety to be imminent. This was explained in the Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000, as follows:

> There is no requirement that the threat be imminent because a threat to public health or public safety, for example, a possible outbreak of infectious disease, may be serious enough to warrant disclosures of personal information but may not be imminent in terms of time. It may be clear that, unless addressed, the threat will do serious harm to public health or safety but unclear when that harm will actually occur.[67]

25.60 The NPPs also permit secondary use and disclosure of an individual's genetic information, if the organisation reasonably believes the use or disclosure to a genetic relative of the individual is necessary to lessen or prevent a serious (but not necessarily imminent) threat to the life, health or safety of a genetic relative of the individual.[68]

25.61 There are additional regimes in the *Privacy Act* to deal with the use and disclosure of personal information in emergencies and disasters. Part VIA of the Act provides a separate regime for the handling of personal information in the event of a declared emergency.[69] Part VIA commenced operation on 7 December 2006.[70] It does not alter the IPPs or NPPs themselves; rather, it displaces some of the requirements in

---

64 See Ch 19, which discusses the meaning and elements of consent.
65 *Privacy Act 1988* (Cth) s 14, IPPs 10(1)(e), 11(1)(c); sch 3, NPP 2.1(e)(i).
66 Ibid sch 3, NPP 2.1(e)(i), (ii).
67 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [356].
68 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(ea). The use and disclosure of genetic information is discussed in Ch 63.
69 The Part VIA regime is discussed in Ch 44.
70 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).

the IPPs and NPPs by providing a separate regime for the collection, use and disclosure of personal information where there is the requisite connection to an emergency that has been the subject of a declaration by the Prime Minister or a minister.

25.62 Finally, the handling of personal information in an emergency or disaster could be the subject of a temporary public interest determination (TPID) made by the Privacy Commissioner under Division 2 of Part VI of the Act.[71]

25.63 This part of the chapter focuses on the operation of the privacy principles in dealing with emergencies or other threats to life that are not declared under Pt VIA, or the subject of a TPID.

Submissions and consultations

25.64 Prior to the release of IP 31, some stakeholders expressed concern about the practical operation of the current principles. The Community Services Ministers' Advisory Council expressed concern that agencies, in endeavouring to protect individuals' privacy, can be unwilling to disclose personal information, which, at times, hampers the protection and care of vulnerable people. The Council stated that it was too difficult to establish that a threat to a person's life or health was both 'serious and imminent' in order to justify a disclosure, stating:

> Other legislation, such as in the child welfare arena, enables the sharing of information when there is 'reasonable suspicion' or concern of abuse and risk. This is a lower threshold, often more appropriate in the case of vulnerable people, and more fitting with the concepts of early intervention and practice.[72]

25.65 In IP 31, the ALRC asked whether agencies and organisations should be permitted expressly to disclose personal information where there is a reasonable belief that disclosure is necessary to prevent a serious and/or imminent threat to any individual's safety or welfare, or a serious threat to public health, public safety or public welfare; and in times of emergency.[73]

25.66 In response to IP 31, a large number of stakeholders submitted that there should be a dilution of the requirement that a threat be *both* imminent *and* serious before personal information can be used or disclosed under the IPPs and NPPs.[74] Reasons for this included that the current provision:

---

71 Temporary public interest determinations are discussed in Ch 47.

72 Community Services Ministers' Advisory Council, *Submission PR 47*, 28 July 2006.

73 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–7(b), (c).

74 For eg, two stakeholders submitted that the threat level should be 'serious *or* imminent', as distinct from 'serious *and* imminent': Australian Federal Police, *Submission PR 186*, 9 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

- operates as a barrier to stop agencies from doing what is necessary to meet 'a credible threat';[75]

- encourages differing interpretations and 'erring on the side of caution, or non-disclosure, in order to protect perceived agency or professional interests (which does not necessarily support the safety of the individuals concerned)';[76] and

- creates a 'catch 22' situation because sometimes a proper assessment of whether a threat is serious and imminent can only be made after the relevant person is aware of the personal information in question.[77]

25.67 A number of stakeholders submitted that the test simply should be whether the threat is 'serious'—that is, the requirement that the threat also be 'imminent' should be removed.[78] Reasons for this included that the imminence requirement:

- creates additional interpretive uncertainty;[79]

- may fuel escalation of a crisis;[80] and

- can be difficult to establish because the information about the extent and nature of a threat is held by another party.[81]

25.68 Some stakeholders preferred a different formulation altogether. Some suggested that the exception should apply where the threat is 'significant', the definition of which may involve balancing the public interest and privacy implications of disclosure.[82] Others proposed greater specificity in the wording of the exception, enabling disclosure where the person reasonably believes it is necessary to protect a child from abuse or neglect.[83]

---

75 Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

76 Government of South Australia, *Submission PR 187*, 12 February 2007.

77 Ibid.

78 Ibid; Confidential, *Submission PR 143*, 24 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 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.

79 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

80 Government of South Australia, *Submission PR 187*, 12 February 2007.

81 Ibid. This stakeholder also noted that removing the 'imminent' element of the exception would enhance consistency across legislation dealing with privacy, secrecy and confidentiality.

82 Confidential, *Submission PR 130*, 17 January 2007. See also Government of South Australia, *Submission PR 187*, 12 February 2007.

83 Confidential, *Submission PR 214*, 27 February 2007. Another stakeholder expressed a similar view: Government of South Australia, *Submission PR 187*, 12 February 2007.

25.69 The OPC favoured the retention of the condition that a relevant threat is to be both serious and imminent. It submitted that the advent of Part VIA and the public interest determination provisions adequately address the concerns about sharing information in emergency situations.[84]

25.70 In DP 72, the ALRC proposed that the 'Use and Disclosure' principle

> should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety.[85]

25.71 In other words, the ALRC proposed:

- removing the requirement that a threat is to be *imminent* in order to claim the benefit of this exception for threats to an individual's life, health or safety; and

- extending to agencies the ability to use and disclose personal information in situations involving serious threats to: an individual's safety, public health or public safety.

25.72 The ALRC expressed the preliminary view that an assessment of whether a threat is serious involves consideration of the gravity of the potential outcome as well as its relative likelihood.[86]

25.73 A majority of stakeholders supported this proposal.[87] Reasons for support included that:

- it would be beneficial for the Department of Defence in satisfying its obligations concerning the health and safety of its personnel;[88]

---

84 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

85 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 22–3.

86 Ibid, [22.61].

87 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; 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 Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. One stakeholder, which supported the proposal, submitted that the exception should be limited to disclosure to law enforcement agencies and emergency service bodies: Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

- the current requirement that a threat should be imminent is too narrow to be effective because it sets a high bar;[89]
- the removal of the imminence requirement will achieve greater clarity;[90]
- it is consistent with confidentiality provisions in social security and family assistance legislation;[91]
- it would assist the Department of Foreign Affairs and Trade (DFAT) in performing its function of providing consular services in situations involving serious threats which are not the subject of a declared emergency;[92] and
- it addresses those situations in which an individual at risk is unable to provide consent to the disclosure of his or her personal information, where such disclosure would benefit that individual.[93]

25.74 The AFP supported the proposal, but stated that it did not address adequately investigations to locate missing persons.[94] Some stakeholders supported the removal of the imminence requirement, but preferred the use of a word other than 'serious'. It also was suggested that any use or disclosure made in good faith for the purpose of protecting an individual's life, health or safety; or public health or safety, should be permitted regardless of the seriousness of the threat.[95]

25.75 The Office of the Victorian Privacy Commissioner agreed that it is arguable that an assessment of whether a threat is serious

> contains within itself an … assessment of the likelihood of a potential negative consequence occurring and the timeframe in which it may occur, together with the extent of damage that would be caused if the consequence eventuated.[96]

25.76 The South Australian Government, however, expressed the view that

> removing the word imminent and solely relying on the word 'serious' does not fully take into account the 'likelihood' of any threat. Therefore, it would seem more appropriate to replace 'imminent' with another term that represents likelihood, but

88 Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.
89 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
90 Ibid.
91 Australian Government Centrelink, *Submission PR 555*, 21 December 2007.
92 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.
93 Ibid.
94 Australian Federal Police, *Submission PR 545*, 24 December 2007. The issue of missing persons is discussed separately below.
95 Confidential, *Submission PR 536*, 21 December 2007. Another stakeholder suggested that the relevant threat should be 'significant': National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.
96 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

> without the implied urgency or immediacy of 'imminent'. For example, 'likely', 'probable', 'anticipated' requires a logical assessment or what may or may not eventuate, and implies a burden of proof. This is consistent with a risk management approach, which generally assesses likelihood as well as consequence.[97]

25.77 A number of stakeholders opposed the removal of the requirement that the relevant threat be imminent.[98] Reasons for this included that:

- many stakeholder concerns are addressed by the amendments to the *Privacy Act* to allow secondary use and disclosure of personal information in emergencies that are the subject of a declaration;[99]
- any broadening of the statutory exception should not be considered until the amendments to the *Privacy Act* concerning declared emergencies have been tested and found to be deficient;[100]
- the imminence test is an important source of privacy protection and removing it would lower privacy protection;[101]
- framing the test solely in terms of a 'serious threat' denies individuals the opportunity to exercise an appropriate degree of control over the disclosure of their personal information;[102]
- a 'serious threat' may create ambiguity and be difficult to apply;[103] and
- 'serious' may not be interpreted as implying a consideration of consequence and likelihood, as suggested in DP 72.[104]

25.78 The Cyberspace Law and Policy Centre submitted the removal of the requirement that the threat be imminent 'would probably be acceptable' for threats to an individual's life, health or safety. It stated, however, that it would be 'very

---

97 Government of South Australia, *Submission PR 565*, 29 January 2008.

98 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Confidential, *Submission PR 535*, 21 December 2007; Optus, *Submission PR 532*, 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. See also M Lander, *Submission PR 451*, 7 December 2007.

99 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

101 See, eg, Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

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

103 Ibid.

104 Ibid. The OPC submitted that if the imminence requirement is removed, 'serious' should be defined to include an assessment of the relative likelihood of the threat eventuating.

dangerous' to remove such a requirement in the context of threats to public health or public safety. It said:

> The first part of the exception is by definition so limited—it will be necessary to identify specific individuals or small groups to satisfy this test. But if the exception was available for public health and public safety without the 'imminent' test, it is difficult to see how claims could not be made under it for a wide range of law enforcement and welfare programmes, including high volume data-matching and data linkage projects. We submit that it was clearly never the intention of Parliament for this exception to provide an alternative basis for such programmes. They should instead have to satisfy one of the other exceptions—typically 'by or under law'.[105]

25.79 As has been noted above, however, there is currently no requirement that a threat to public health or safety be imminent. This was the express intention of Parliament.[106]

25.80 The OPC expressed concern about authorising the use and disclosure of personal information to address threats to safety. It stated that

> retaining 'safety' in addition to 'life or health' may create scope for uses and disclosures in wider circumstances than originally intended. It may, for instance, be used to justify uses and disclosures for unspecified, or poorly-defined threats.[107]

25.81 The OPC also submitted that if the imminence requirement is removed, the relevant provision should require that where there is a serious threat, the agency or organisation should seek the consent of the individual where reasonably practicable.[108]

ALRC's view

25.82 Agencies and organisations should be permitted to use and disclose personal information for a purpose other than the primary purpose of collection if they reasonably believe that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety; or public health or safety.

25.83 The current requirement that the requisite threats to an individual be imminent as well as serious sets a disproportionately high bar to the use and disclosure of personal information. This is problematic in circumstances in which there may be compelling policy reasons for the information to be used or disclosed but it is impracticable to seek consent. Agencies and organisations should be able to take preventative action to stop a threat from escalating to the point of materialisation. In order to do so, they may need to use or disclose personal information.

---

105 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
106 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 143–144.
107 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
108 Ibid.

25.84 The requirement that the requisite threats to an individual be imminent, therefore, should be removed. Any analysis of whether a threat is 'serious' must involve consideration of the gravity of the potential outcome as well as the relative likelihood. If a threat carries a potentially grave outcome but is highly unlikely to occur, it cannot be considered 'serious' in any meaningful sense. The word 'serious' cannot be considered in isolation. It must be considered in the context of a 'serious threat'. The second listed definition of 'threat' in the *Macquarie Dictionary* is 'an indication of *probable* evil to come'.[109] This indicates that an assessment of likelihood of harm is implied.

25.85 While the removal of the imminence requirement will not impact on the need to assess *whether* a threat is likely to eventuate, it will render unnecessary an assessment of *when* a threat is likely to take place. This is borne out by the definition of 'imminent', which focuses on the immediacy of a threat. The *Macquarie Dictionary* defines 'imminent' as 'likely to occur *at any moment*; impending'.[110] It defines 'impending' as '*about to happen*; imminent'.[111]

25.86 It should be emphasised that there are important safeguards contained in the formulation of the exception recommended by the ALRC. In each case, an agency or organisation will need to form a reasonable belief that the use or disclosure is necessary to lessen or prevent the requisite threat. An agency or organisation, therefore, will need to have reasonable grounds for its belief that the proposed use or disclosure is essential, and not merely helpful, desirable, or convenient.

25.87 There is a strong public interest in averting threats to life, health and safety. To remove the categories of threat relating to an individual's safety or public safety, as suggested by one stakeholder, would leave a gap in the operation of the principles, and potentially lead to ambiguity in their application. For example, if an individual is facing a serious risk of injury or danger, in the absence of an exception allowing use and disclosure to prevent serious threats to safety, an agency or organisation may take an overly-conservative view that such risks do not constitute either a threat to life or health, and therefore refrain from acting.

109 *Macquarie Dictionary* (online ed, 2007), (emphasis added).
110 Ibid, (emphasis added).
111 Ibid, (emphasis added).

Recommendation 25–3 The 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose other than the primary purpose of collection (the secondary purpose) if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety.

Reason to suspect unlawful activity

25.88 NPP 2.1(f) allows secondary use or disclosure of personal information by an organisation if it

> 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.[112]

25.89 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 stated that:

> This sub-principle explicitly acknowledges that one of an organisation's legitimate functions is to investigate, and report on, suspected unlawful activity relating to its operations. [113]

25.90 The OPC's guidance on this exception states that 'ordinarily but not in all cases, the suspected unlawful activity would relate to the organisation's operations'.[114] The OPC also has stated that it will be a 'necessary' part of an organisation's investigations where it cannot effectively investigate or report the suspected unlawful activity without using or disclosing the information.[115]

25.91 'Investigation' has been interpreted to include

> the internal handling of complaints or allegations regarding professional misconduct, sexual harassment or assault and the reporting of them to the police or another relevant person or authority.[116]

---

112 *Privacy Act 1988* (Cth) sch 3, NPP2.1(f).
113 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [357].
114 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41.
115 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001), 2.
116 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 19.

25.92 The IPPs do not contain an equivalent exception.

Submissions and consultations

25.93 In DP 72, the ALRC included in its draft 'Use and Disclosure' principle an exception to the general prohibition on secondary use and disclosure of personal information, relating to reasonable suspicion of unlawful activity.[117] This exception was based on the one contained in NPP 2.1(f). In effect, the ALRC proposed extending this exception to the public sector.

25.94 Stakeholders did not express opposition to the proposed extension.[118] The DFAT stated that the proposed exception would 'assist the Department to pass on information to the relevant authorities where necessary'.[119]

25.95 DFAT and Centrelink each submitted, however, that the exception should be expanded to include investigations of serious misconduct[120]—for example, breaches of the *Australian Public Service Code of Conduct*.[121] DFAT also submitted that it would

> support an interpretation of 'unlawful activity' in UPP 5.1(d) as including activities in breach not only of Australian law, but also foreign laws and international law (for example, as set out in international instruments and bilateral agreements to which Australia is a party).[122]

25.96 The OPC suggested that consideration be given to defining more precisely legitimate uses and disclosures for the purpose of investigating alleged unlawful activity. It noted that the 'relevant persons or authorities' referred to in the exception are not 'identified as being explicitly linked to the investigation', which could lead to overly broad interpretations. The OPC suggested that the exception could refer simply to disclosure necessary for investigations or proceedings concerning the matter. Alternatively, it stated that consideration could be given to including, within the principle, a non-exhaustive list of persons who, and authorities that, would fall within the exception.[123]

ALRC's view

25.97 The 'Use and Disclosure' principle should contain an exception authorising the use or disclosure of personal information by agencies and organisations where they have reason to suspect unlawful activity has been, is being, or may be, engaged in. This

---

117 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), UPP 5.1(d).

118 The Cyberspace Law and Policy Centre supported it expressly: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

119 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.

120 Ibid; Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

121 Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

122 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.

123 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001) lists the bodies considered by the OPC to fall within the scope of the exception.

exception should apply only if such use or disclosure is a necessary part of an agency's or organisation's investigation of the matter or in reporting its concerns to relevant persons or authorities.[124]

25.98 It is unnecessary to expand the scope of this exception to include expressly investigations of serious misconduct. The OPC's guidance on 'investigation' interprets 'investigation' to include investigation of professional misconduct. In addition, and more significantly, another exception in the model 'Use and Disclosure' principle authorises use and disclosure of personal information if an agency or organisation reasonably believes it is necessary by or on behalf of an enforcement body to prevent, detect, investigate or remedy serious misconduct.[125] This exception is discussed further below.

Required or authorised by or under law

25.99 NPP 2.1(g) and IPPs 10.1(c) and 11.1(d) permit use or disclosure where this is 'required or authorised by or under law'.[126] The Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 stated that:

> The sub-principle [NPP 2.1(g)] is intended to cover situations where a law unambiguously requires or authorises the use or disclosure of personal information. There could be situations where the law requires some actions which, of necessity, involve particular uses or disclosures, but this sort of implied requirement would be conservatively interpreted. The reference to 'authorised' encompasses circumstances where the law permits, but does not require, use or disclosure.[127]

25.100 The OPC's guidance on NPP 2.1(g) provides:

> The *Privacy Act* does not override specific legal obligations relating to use or disclosure of personal information … If an organisation is required by law to use or disclose personal information it has no choice and it must do so. If an organisation is authorised by law to use or disclose personal information it means the organisation can decide whether to do so or not.[128]

25.101 In response to IP 31, the OPC suggested that this exception should be narrowed with respect to the use or disclosure of sensitive information. It submitted that, 'to avoid a broad reading of this [exception] where sensitive information is at stake, the inclusion of "clearly" or "expressly" authorised could be considered'.[129]

---

124 The concerns about the precise drafting of the exception and, in particular, whether the exception should contain a non-exhaustive list of relevant persons and authorities that fall within the scope of the exception will best be addressed by the Office of Parliamentary Counsel.

125 An 'enforcement body' is defined in s 6 of the *Privacy Act*. It includes, for example, the Australian Federal Police, the Integrity Commissioner, and agencies to the extent that they are responsible for administering law relating to the protection of the public revenue.

126 The meaning of 'required or authorised by or under law' is discussed in detail in Ch 16.

127 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [336].

128 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41.

129 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

25.102 In DP 72, the ALRC asked the following question:

> Should the proposed 'Use and Disclosure' principle contain an exception allowing an agency or organisation to use or disclose personal information for a purpose other than the primary purpose of collection where this is 'required or *specifically* authorised by or under law' instead of simply 'required or authorised by or under law'?[130]

Submissions and consultations

25.103 Stakeholders' opinions were divided on whether use and disclosure under this limb should be specifically required or authorised by or under law. A number of stakeholders, including privacy advocates and privacy commissioners, supported such an approach.[131] Some stakeholders stated that requiring specific authorisation would promote clarity of approach.[132] For example, GE Money stated:

> Organisations receive very many requests for disclosure of information to a wide range of government agencies. Many hours are spent debating with those agencies whether the organisation is currently required to provide the information. Much criticism is directed at organisations for the 'risk averse' approach taken to these sorts of considerations. GE considers it appropriate that where third parties require access to information that they are unambiguously empowered to require it before an organisation should provide it.[133]

25.104 PIAC expressed the view that the narrowing of the exception is justified 'given the high degree of public concern about use of personal information for purposes other than its original purpose'.[134] Privacy NSW stated that in its experience, New South Wales agencies tend to overstate the authority granted by the relevant law.[135]

25.105 A large number of stakeholders opposed a requirement for a use or disclosure to be specifically authorised by or under law.[136] Concerns included that a requirement for 'specific' authorisation:

---

130 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 22–1.

131 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; GE Money Australia, *Submission PR 537,* 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; I Graham, *Submission PR 427,* 9 December 2007.

132 GE Money Australia, *Submission PR 537,* 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.

133 GE Money Australia, *Submission PR 537,* 21 December 2007.

134 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

135 Privacy NSW, *Submission PR 468,* 14 December 2007.

136 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; Australian Government Centrelink, *Submission PR 555,* 21 December 2007; Australian Federal Police, *Submission PR 545,* 24 December 2007; Confidential, *Submission PR 536,* 21 December 2007; Medicare Australia, *Submission PR 534,* 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525,* 21 December 2007; Australian Taxation Office, *Submission PR 515,* 21 December 2007; Australian Collectors Association,

- is superfluous[137] and unnecessary because: 'a use or disclosure is either authorised or is not authorised by or under law';[138] or the current approach strikes an appropriate balance between facilitating the efficient operations of an agency and protecting the privacy of individuals;[139]

- does not take into account adequately the nature of many federal laws on disclosure;[140]

- assumes that all of the powers and functions of an agency always will be set out expressly in legislation, when in fact, what is required may be determined by necessary implication;[141]

- will have the unintended consequence of preventing the release of personal information when a 'fair reading' of the law authorises disclosure by implication;[142]

- may not cater for circumstances in which use or disclosure may be authorised by a contractual duty,[143] duty of care,[144] a statutory duty not to mislead or deceive,[145] or the common law duty of confidentiality;[146] and

---

Submission PR 505, 20 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. See also National Australia Bank, *Submission PR 408*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007, which expressed concerns about such an approach. See also Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008 which expressed support for retention of the current approach.

137 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

138 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

139 Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

140 Australian Taxation Office, *Submission PR 515*, 21 December 2007.

141 Australian Federal Police, *Submission PR 545*, 24 December 2007. Similarly, the ATO expressed concern that the requirement will potentially be interpreted narrowly to mean 'express' authorisation: Australian Taxation Office, *Submission PR 515*, 21 December 2007.

142 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007. See also Australian Taxation Office, *Submission PR 515*, 21 December 2007, which expressed the similar view that such an approach could 'compromise disclosures which Parliament clearly intended could be made'.

143 Australian Collectors Association, *Submission PR 505*, 20 December 2007. See also Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

144 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

145 Ibid.

146 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

- would necessitate an amendment to existing legislation which was not drafted with such a requirement in mind.[147]

ALRC's view

25.106 The 'Use and Disclosure' principle must contain an exception which allows for the legitimate use and disclosure of personal information if it is required or authorised by or under law. To impose a restriction that may narrow the scope of the exception to express legislative authorisations only is likely to have far-reaching, and possibly unintended, consequences. For example, it may impact negatively on the ability of agencies to fulfil their statutory functions and exercise their powers. It may compromise disclosures which, by necessary implication, parliament intended to be made. Imposing a 'specific authorisation' requirement also would likely necessitate a review of current legislation to ensure that, where needed, the use and disclosure of personal information is specifically authorised.

25.107 Promoting clarity of approach was a key factor cited by those stakeholders that supported a requirement for specific authorisation. Increased clarity, however, is likely to be achieved if the ALRC's recommendations on the 'required or authorised by or under law' exception are implemented. As discussed in Chapter 16, the ALRC has recommended that the *Privacy Act* should be amended to set out what 'law' includes for the purpose of the exception.[148] It also has recommended that the OPC should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law.[149]

25.108 Absent a legislative requirement that a use or disclosure for a secondary purpose must be specifically authorised, agencies and organisations must nonetheless be able to establish the basis upon which they assert their entitlement to rely on the exception. That is, they will still need to be able to identify the law which they assert requires or authorises a particular use or disclosure.

25.109 It is unnecessary and undesirable, therefore, for privacy legislation to mandate that a use or disclosure of personal information for a secondary purpose must be specifically authorised by or under law in order to qualify as a permitted exception to the prohibition on such use and disclosure.

Law enforcement and regulatory purposes

25.110 IPPs 10 and 11, respectively, permit agencies to use personal information for a secondary purpose, and to disclose personal information where use or disclosure is

147 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; National Australia Bank, *Submission PR 408*, 7 December 2007.
148 See Rec 16–1.
149 See Rec 16–2.

'reasonably necessary for enforcement of the criminal law, a law imposing a pecuniary penalty, or for the protection of the public revenue'.[150]

25.111 NPP 2.1(h) allows an organisation to use or disclose personal information for a secondary purpose if it

> reasonably believes it is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
>
> (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
>
> (ii) the enforcement of laws relating to the proceeds of crime;
>
> (iii) the protection of the public revenue;
>
> (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;[151]
>
> (v) the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of the orders of a court or tribunal.[152]

25.112 The OPC has issued an Information Sheet which provides guidance on this exception.[153] For example, that guidance provides that:

> 'Seriously improper conduct' refers to serious breaches of standards of conduct associated with a person's duties, powers, authority and responsibilities. It includes corruption, abuse of power, dereliction of duty, breach of obligations that would warrant the taking of enforcement action by an enforcement body or any other seriously reprehensible behaviour.[154]

Submissions and consultations

25.113 In DP 72, the ALRC, based on its use of the NPPs as a template, included in its draft 'Use and Disclosure' principle an exception to the general prohibition on secondary use and disclosure of personal information based substantially on the law

---

150 *Privacy Act 1988* (Cth) s 14, IPP 10.1(d), IPP 11.1(e). See 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), Guidelines 39–41, for the OPC's interpretation of 'enforce the criminal law'; 'enforce a law imposing a pecuniary penalty' and 'protect the public revenue'.

151 IPP 11 does not contain a direct equivalent of this limb. In Privacy Commissioner, *Public Interest Determination 3A*, 22 August 1991, the Privacy Commissioner allowed the Director of Public Prosecutions 'to disclose to a relevant authority information in its possession about an individual where that information indicates serious misconduct directly relevant to the performance of a regulated occupation or profession; or of a public service position'.

152 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(h). 'Enforcement body' is defined in s 6 of the *Privacy Act*.

153 See Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001).

154 Ibid, 3.

enforcement exception contained in NPP 2.1(h).[155] This had the effect of consolidating the approach to the law enforcement exception to both the private and public sectors.

25.114 The Cyberspace Law and Policy Centre supported this approach expressly.[156] It also submitted that a note to the exception should state that it 'requires the active involvement' of an enforcement body, that is:

> it should not be open for an agency or organisation to claim this exception in respect of uses and disclosures which [are] only of prospective interest to an enforcement body.[157]

25.115 One stakeholder expressed concern that the proposed exception may not address adequately the intelligence-gathering functions of agencies and their need to share criminal information and intelligence.[158]

ALRC's view

25.116 The 'Use and Disclosure' principle should contain an exception permitting agencies and organisations to use and disclose personal information for a secondary purpose if they reasonably believe it is necessary for, or on behalf of, an enforcement body to perform one of the functions specified in NPP 2.1(h).

25.117 The law enforcement exception contained in the NPPs is to be preferred to that contained in the IPPs because of its greater scope. It canvasses with greater precision the legitimate areas of law enforcement and regulation that warrant the authorisation of secondary use and disclosure of personal information. It also promotes clarity.

25.118 The law enforcement exception should not be limited to circumstances in which there is an 'active' involvement of an enforcement body, as suggested by two stakeholders. Such a provision would be counter-productive, potentially limiting the operation of the law enforcement exception to allowing use and disclosure of personal information to assist law enforcement bodies to undertake *existing* investigations into offences and breaches of the law. A law enforcement body, however, may not be in a position to prevent, detect or investigate offences or breaches of the law, unless and until certain information, including personal information, is brought to its attention. The exception, therefore, should not be framed in a manner that prejudices the ability of enforcement agencies to *initiate* investigations in the public interest.

25.119 It is not necessary to amend the law enforcement exception to address specifically the intelligence-gathering functions of agencies. The OPC's guidance on the use and disclosure principles in the IPPs takes a purposive approach and

---

155 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), UPP 5.1(f).
156 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
157 Ibid. Another stakeholder expressed a similar view: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
158 Confidential, *Submission PR 488*, 19 December 2007.

acknowledges specifically that an agency may need to use and disclose personal information for intelligence-gathering that does not relate to a specific crime. It provides that:

> In safeguarding one of the public purposes listed in exceptions 10.1(d) or IPP 11.1(e), it may be reasonably necessary for an agency to use or disclose information about a range of people—even though none of them has yet been directly linked to an unlawful activity.
>
> *For example*: Investigators may suspect that an particular building is being used in drug trafficking and may think it reasonably necessary for enforcing the criminal law that they gather information about people associated with the building—even though they do not know what part, if any, those people play in the suspected activity.[159]

Research

25.120 NPP 2.1(d) provides that an organisation may use or disclose health information where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety where:

- 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;[160] and
- 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.

25.121 In Chapter 65, the ALRC has recommended expanding the scope of the research exception beyond health and medical research to apply to human research generally.[161] The ALRC has recommended specific conditions upon which use and disclosure necessary for research is to be authorised.[162] The 'Use and Disclosure' principle set out at the end of this chapter, therefore, contains the recommended research exception.[163]

---

159 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), 46.

160 Section 95A of the *Privacy Act* allows the Commissioner to approve, for the purposes of the NPPs, guidelines that are issued by the CEO of the National Health and Medical Research Council or a prescribed authority. See discussion in Part H.

161 See Rec 65–2.

162 See Rec 65–9.

163 The discussion supporting the inclusion of this exception is in Ch 65.

Provision of a health service

25.122 NPP 2.4 permits an organisation that provides a health service to an individual to disclose health information about the individual to a person who is responsible for the individual if certain conditions are met. NPPs 2.5 and 2.6 define a person responsible for an individual.[164]

25.123 The ALRC has recommended that NPPs 2.4 to 2.6 should be moved to the new *Privacy (Health Information) Regulations*.[165] Those provisions, therefore, are not included in the 'Use and Disclosure' principle. The ALRC also has recommended that the new regulations should provide that 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.[166]

Genetic information

25.124 NPP 2.1(ea) contains an exception to the general prohibition on the use and disclosure of personal information for a secondary purpose that authorises the use and disclosure of genetic information obtained in the course of providing a health service to an individual. This is allowed where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative of the individual. This exception is discussed in Chapter 63.

25.125 The ALRC has recommended that this specific exception should be moved out of the 'Use and Disclosure' principle and be dealt with in the new *Privacy (Health Information) Regulations*.[167] These regulations are to apply to both agencies and organisations.[168]

Confidential alternative dispute resolution process

25.126 Neither the NPPs or the IPPs contain an exception authorising a secondary use or disclosure of personal information where it is necessary for the purpose of a confidential alternative dispute resolution process. For the reasons discussed in detail in Chapter 44, the 'Use and Disclosure' principle should contain such an exception.

---

164 These provisions are discussed more fully in Ch 63.
165 See Rec 63–3.
166 See Rec 63–3.
167 See Rec 63–5.
168 See Rec 63–5.

Additional exceptions?

Missing persons

25.127 Concern has been expressed that the IPPs and NPPs do not cover adequately the disclosure of personal information to law enforcement authorities, and the use of the information by them, when undertaking functions that do not or may not involve a criminal offence or breach of the law but are nevertheless in the public interest.[169] The typical example of this is missing person investigations by the police and others. In contrast, Tasmanian privacy legislation expressly allows the use and disclosure of personal information where the secondary purpose is the investigation of missing persons by a law enforcement agency.[170]

25.128 The OPC review of the private sector provisions of the *Privacy Act* (OPC Review) noted that stakeholders did not generally call for a change to the NPPs in the law enforcement context. It stated that 'generally, it appears the construction of the law is considered to be reasonable, but problems seem to arise in its application'.[171] The OPC stated that it would work with the law enforcement community, private sector bodies and community representatives to develop practical guidance to assist private sector organisations in understanding their obligations under the *Privacy Act*.[172]

25.129 In its submission to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry), the AFP noted that, while education may have a role to play in raising awareness, it was unlikely to offer a complete solution. It submitted that a possible solution might be to give it the power to issue a notice to produce.[173] The Senate Committee privacy inquiry supported the OPC's recommendation to develop practical guidance in this area, but considered that the Australian Government also should consider additional mechanisms to resolve the issue.[174]

Submissions and consultations

25.130 In IP 31, the ALRC asked whether agencies and organisations should be permitted expressly to disclose personal information to assist in the investigation of missing persons.[175] In response to IP 31, a number of stakeholders supported such an

---

169 See Department of Foreign Affairs and Trade, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 8 March 2005.

170 *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(1)(g)(vi).

171 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 223.

172 Ibid, rec 65.

173 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.119], [5.121].

174 Ibid, [7.52].

175 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–7(a).

amendment.[176] CrimTrac, for example, submitted that it is sometimes necessary for police to share information such as criminal records to assist in searching for missing persons.[177]

25.131 The AFP noted the difficulties that police have in accessing information about missing persons. It stated that:

> Police action to locate missing persons may not involve the enforcement of a criminal law, may not always be necessary to prevent or lessen serious and imminent threat to life or health, the person is unlikely to have consented to the information being disclosed for this purpose nor would it be reasonably likely that [he or she would be] aware the information would be disclosed to police … This situation arguably means that the *Privacy Act* currently denies a missing person the knowledge or right to know that their relatives and friends are looking for them. The *Privacy Act* should authorise police and relevant non government organisations to access personal information that constitutes evidence of life so that police or these other agencies can locate the missing person, secure their safety if necessary and give them the option of re-uniting with their family and friends.[178]

25.132 Major Kathy Smith of the Salvation Army Family Tracing Service (South Australia) submitted that the *Privacy Act* should be amended to allow the Service to be 'given information or confirmation of the whereabouts of the person [it is] looking for', given its role in reuniting family members who have become separated.[179]

25.133 The Office of the Information Commissioner (Northern Territory), however, expressed concern about amending the privacy principles to authorise unconditionally disclosures to organisations to assist them in missing person investigations. The Office noted that it had issued two Grants of Authorisation for Northern Territory agencies to assist a private sector organisation to search for missing persons.[180]

25.134 The Institute of Mercantile Agents suggested a more extensive amendment to permit all private and public sector entities that deal with missing persons to 'have regulated and audited access to locator information'. In particular, it stated that its members should have access to such information because 'the costs of missing persons not meeting their obligations' amounts to at least four billion dollars annually.[181]

---

176 CrimTrac, *Submission PR 158*, 31 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.

177 CrimTrac, *Submission PR 158*, 31 January 2007.

178 Australian Federal Police, *Submission PR 186*, 9 February 2007.

179 K Smith, *Submission PR 246*, 8 March 2007. See also Salvation Army, *Submission PR 15*, 2 June 2006.

180 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007. The decisions granting those authorisations are available at http://www/nt.gov.au/justice/infocomm/publications/decisions.shtml (Grants of Authorisation 1 and 2 of 2005).

181 Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.

25.135 Other stakeholders opposed any change to the privacy principles in respect of missing persons, noting that sometimes a missing person has committed no offence and does not wish to be located.[182] The OPC submitted that:

> The current exceptions in NPP 2 and IPPs 10 and 11 of the *Privacy Act* are adequate, achieve the right balance and are appropriate for the circumstances of a missing person. The Office acknowledges that there may be circumstances where an individual may choose not to remain in contact with the people they know and believes that allowing the disclosure of personal information generally for the use in locating missing persons would adversely impact upon the privacy rights of those individuals. Further, the Office notes that the Commissioner's power to make Public Interest Determinations (PIDs) provide a mechanism to deal with possible circumstances in which the provisions are not adequate.[183]

25.136 The ATO stated:

> We would have some reservations … about disclosing information in the case of a missing person. In some situations, such as family breakdown or domestic violence, there may be a report of a missing person, but it is difficult to determine whether the person is in fact 'missing' or has chosen to move away for another reason.[184]

25.137 In DP 72, the ALRC expressed the preliminary view that the privacy principles do not need to be amended to allow expressly agencies and organisations to use or disclose personal information to assist in the investigation of missing persons.[185] Privacy advocates expressed support for this view.[186] The OPC also supported this approach. It submitted that the area of missing persons investigations 'may not be one which can be completely resolved through amendments within the parameters of the *Privacy Act* itself'.[187]

25.138 The AFP, however, submitted in response to the ALRC's proposal to remove the requirement that a threat to an individual's life, health or safety be imminent,[188] that this did not address adequately missing persons investigations. It provided the following example to illustrate a situation that it submitted would justify the creation of an exception relating to missing persons:

> A young man goes missing due to psychological health issues and becomes disconnected from his significant relationships. He is unaware that his family have

---

182 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Taxation Office, *Submission PR 168*, 15 February 2007.

183 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. Public interest determinations are discussed in Ch 47.

184 Australian Taxation Office, *Submission PR 168*, 15 February 2007.

185 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [22.76]–[22.79].

186 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

188 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 22–3, which is discussed above.

> lodged a missing persons report. The longer he is away from his support network the harder it is to make contact, particularly without knowing that a missing persons report has been made …
>
> If personal information is disclosed and the person is located by police, they then have the right to choose whether they have contact with their family or not. At the very least the Police may be able to assist the young man in re-establishing his contacts that may have a flow on effect in benefiting his mental health and general wellbeing.[189]

ALRC's view

25.139 Authorising the disclosure of personal information to assist in missing persons investigations raises complex issues and competing policy considerations. Those involved in seeking to locate missing persons may be assisted by an express exception in the *Privacy Act*, authorising disclosure. In some cases, an express authorisation may assist in locating missing persons, and in delivering positive results where the missing persons want to be located.

25.140 On the other hand, the creation of an express exception may result in adverse consequences in cases where missing persons do not wish to be located. As a number of stakeholders pointed out, sometimes missing persons have not committed an offence and may be seeking to hide—not from the authorities but from others. For example, individuals for personal reasons may choose to disassociate themselves from family and friends, or may seek to conceal their whereabouts in order to protect their safety. Examples of the latter are where an individual has fled from a violent relationship, or has witnessed a violent crime and fears retaliation. To create a general exception in respect of all missing person investigations risks interfering with the privacy of certain missing individuals and, possibly, endangering their lives.

25.141 On balance, therefore, it is undesirable for a new exception to the 'Use and Disclosure' principle to be created to allow expressly for disclosure of personal information to assist in missing persons investigations. Where an agency or organisation has a legitimate reason to search for a missing person, it may be able to avail itself of one of the other exceptions to the general prohibition in the 'Use and Disclosure' principle, or it may seek a public interest determination.[190]

25.142 Some of the ALRC's recommendations concerning other exceptions in the 'Use and Disclosure' principle, if implemented, would assist in broadening the scope of situations in which disclosure of personal information in missing persons investigations would be authorised. In particular, the ALRC's recommendation that agencies and organisations should be authorised to use or disclose personal information where there is a serious threat to an individual's life, health or safety would allow the disclosure of personal information in some missing persons investigations.[191] The fact

---

189 Australian Federal Police, *Submission PR 545*, 24 December 2007.
190 Public interest determinations are discussed in Ch 47.
191 See Rec 25–3.

that agencies and organisations would no longer need to establish that the threat to a missing individual is imminent will increase the likelihood of the applicability of the exception.

25.143 Depending on the circumstances of a matter, the law enforcement exception in the 'Use and Disclosure' principle also may serve to authorise the disclosure of personal information in a missing person investigation.

Disclosure of 'incidents' by insured professionals to insurers

25.144 Insured professionals may need to disclose 'incidents' to their insurers, such as those that may result in an action for damages for negligence. For example, a doctor may need to disclose the existence of an incident to his or her insurer so that the insurer can assess the legal risk and make financial provision for a possible future claim. The incident may or may not mature into a legal claim. While disclosure of the doctor's personal information to the insurer occurs with consent, the legality of the disclosure of the patient's personal information is likely to be less clear, needing to be justified pursuant to another exception to the use and disclosure principle.

25.145 NPP 2.1(a) could be relied upon in the above circumstances. If the disclosure involves health information, which is sensitive information, the purpose of providing advice in relation to indemnity will have to be 'directly related' to the primary purpose of collection of the patient's information—generally being the care and treatment of the patient. In addition, NPP 2.1(a) requires that the individual would reasonably expect the doctor to disclose his or her personal information to the doctor's insurer following an incident.[192] Many patients may not have considered this.

25.146 The OPC has issued guidelines on the application of the privacy principles to the private health sector. These guidelines make it clear, therefore, that disclosures of incidents to insurers:

- are covered in the 'directly related' limb of the exception in specified circumstances, and
- may fall within the reasonable expectations of an individual.[193]

25.147 In addition, disclosure of incidents to insurers may fall within the 'required or authorised by or under law' exception. For example, under s 21 of the *Insurance Contracts Act 1984* (Cth), an insured has a duty to disclosure to the insurer before the contract of insurance is entered into, every matter known to the insured, that:

---

192 The exception in NPP 2.1(a) is reproduced in the 'Use and Disclosure' principle, at UPP 5.1(a).

193 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001).

- the insured knows to be a matter relevant to the decision of the insurer whether to accept the risk and, if so, on what terms; or

- a reasonable person in the circumstances could be expected to know to be a relevant matter.

Submissions and consultations

25.148 In IP 31, the ALRC asked whether the exceptions in NPP 2 are adequate to cover: (a) disclosures by a professional of a client's personal information pursuant to an indemnity insurance contract where the provision of professional services has led to an adverse outcome; and (b) on-disclosures by insurers to members of their 'cases committees', often comprising experts in the relevant profession, who advise insurers about making provision for possible future claims.[194]

25.149 In response to IP 31, UNITED Medical Protection submitted that disclosure of incidents to insurers would either fall within the ambit of NPP 2.1(a) (related or directly related purpose and within reasonable expectations of individual) or NPP 2.1 (g) (required or authorised by or under law). Nonetheless, UNITED Medical Protection submitted that, in the interests of clarity, an exception to the 'Use and Disclosure' principle should be created to allow professionals to make disclosures to their professional indemnity insurers, or the matter should be dealt with by way of public interest determination.[195] Similarly, the Australian Bankers' Association suggested that the best solution would be to create an express exception to the general prohibition against use and disclosure for a secondary purpose 'to allow for disclosure of incidents to insurers'.[196]

25.150 In DP 72, the ALRC expressed the preliminary view that it is unnecessary to amend the 'Use and Disclosure' principle to provide for an express exception authorising the disclosure of incidents by insured professionals.[197] The OPC and the Cyberspace Law and Policy Centre supported expressly the view that such an exception is unnecessary.[198]

ALRC's view

25.151 It is unnecessary to create a new exception to the 'Use and Disclosure' principle to allow for the notification of incidents by professionals to insurers. Disclosures of this nature may be authorised by existing exceptions to the 'Use and Disclosure' principle, namely:

---

194 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.84].
195 UNITED Medical Protection, *Submission PR 118*, 15 January 2007.
196 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007. See also National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.
197 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [22.87]–[22.91].
198 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

- if the individual affected has consented to the disclosure;
- if the disclosure is required or authorised by or under law; or
- in circumstances where: there is a relation, or, in the case of sensitive information, a direct relation between the disclosure and the primary purpose of collection; and the disclosure is within the reasonable expectations of the individual.[199]

25.152 Relevant professional bodies should educate their clients about the need for professionals to disclose incidents to insurers. Raising awareness in this area will increase the likelihood that such disclosures will fall within the reasonable expectations of individuals. Education will play a key part in obviating any perceived need for a discrete exception in this regard.

Due diligence

25.153 A prospective purchaser of a business undertakes a process of due diligence to assess the value of the business's assets and liabilities. This process may involve the collection and disclosure of personal information about employees, customers, trading partners and business associates. An issue raised in the OPC Review was whether the practice of due diligence on the sale and purchase of a business raises any particular privacy concerns.[200] The issue of due diligence in the context of mergers and acquisitions has also been raised in this Inquiry.[201]

25.154 In 2002, the OPC issued an information sheet concerning the application of key NPPs to due diligence when buying and selling a business.[202] The information sheet provides expressly that:

> Personal information may be disclosed by a vendor of a business … to prospective purchasers of that business … for the purpose of due diligence investigations. Such disclosure will occur before the sale has been completed.[203]

25.155 In the OPC Review, the OPC reported that it had not received a complaint about a breach of privacy during a due diligence exercise. It stated that it is not practical to require an organisation in the process of due diligence to gain the consent of everyone whose personal information is transferred and it recommended that the Australian Government should consider amending the NPPs to take into account the

---

199 See UPP 5.1(a).
200 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), [6.11].
201 G Hill, *Consultation PC 21*, Melbourne, 8 May 2006.
202 Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002).
203 Ibid, 1.

practice of due diligence.[204] New Zealand law, for instance, allows disclosure of information where 'it is necessary to facilitate the sale or other disposition of a business as a going concern'.[205]

25.156 In IP 31, the ALRC solicited views as to whether the privacy principles needed to be amended to allow for the disclosure of personal information during the course of due diligence. The ALRC also asked whether there is a need to amend Information Sheet 16 in this regard.[206] Only the Queensland Council for Civil Liberties made a submission on this issue. It stated:

> We are not sure whether on a flexible and pragmatic approach to the privacy principles that due diligence actually raises serious privacy issues. However, if it is a serious concern, then a relevant amendment should be made.[207]

25.157 In DP 72, the ALRC expressed the preliminary view that there is no need to create a new exception to the 'Use and Disclosure' principle dealing with the use and disclosure of personal information in the course of due diligence.[208] The OPC and privacy advocates expressly supported the ALRC's view.[209]

ALRC's view

25.158 No need has been demonstrated to create a new exception to the 'Use and Disclosure' principle dealing with the use and disclosure of personal information in the course of due diligence. The fact that very few stakeholders identified a problem suggests that the use and disclosure principles are being applied in a flexible and pragmatic manner in this area. Moreover, the OPC's guidance on this issue takes a purposive approach, acknowledging expressly that disclosure for the purpose of due diligence is authorised.

Legal advice and proceedings

25.159 Neither the IPPs nor the NPPs provide expressly for the use and disclosure of personal information for the purpose of obtaining legal advice or for use in legal proceedings. There is precedent, however, for such an approach in the privacy legislation of other jurisdictions.[210]

---

204 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 191 and rec 57.

205 *Privacy Act 1993* (NZ) s 6, Principle 11.

206 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.106]–[4.107].

207 Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

208 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [22.99]–[22.100].

209 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.

210 See, eg, *Data Protection Act 1998* (UK) s 35(2); *Privacy Act 1993* (NZ) s 6, Principle 10(c)(iv); Principle 11(e)(iv). The relevant provision in the UK legislation is set out in Ch 44. See Ch 44 also for a general discussion on obtaining personal information from third parties for the purpose of pursuing or defending legal claims.

25.160 IP 31 and DP 72 did not address the issue of whether there needed to be an express exception to the privacy principles relating to legal advice and legal proceedings. Following the release of DP 72, however, Avant Mutual Group Ltd stated that:

> Proposed UPP 5 does not provide an exemption from the non-disclosure provisions for providing legal advice and for legal services in anticipation of and/or for actual legal proceedings whether before a court, tribunal or statutory authority …
>
> Proposed UPP 2.6(e) allows collection where it 'is necessary for the establishment, exercise or defence of a legal or equitable claim'. Furthermore proposed UPP 9(d) allows objection to be taken to access when the documents were created for anticipated or actual legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery in the proceedings.
>
> Avant submits that consistency requires that if an organisation is rightly able to collect information for the establishment, exercise or defence of a legal or equitable claim there should be a corresponding ability to disclose or use information to legal advisers and third parties such as independent experts for the same purpose. However … the term 'establishment, exercise or defence of a legal or equitable claim' is too narrow and use and disclosure should be permissible in order to obtain legal advice and for legal services provided in anticipation of and/or for actual proceedings before a Court, Tribunal or Statutory Authority.[211]

ALRC's view

25.161 It appears to be unnecessary to amend the 'Use and Disclosure' principle to provide an express exception relating to use and disclosure of personal information for the purposes of obtaining legal advice or for use in legal proceedings. This view is based on two main reasons. First, depending on the circumstances, other exceptions in the 'Use and Disclosure' principle, which are addressed below, can be relied upon to authorise such use or disclosure. Secondly, the OPC has taken a purposive and pragmatic approach in its interpretation of the privacy principles in this area. If the OPC were to change its purposive approach, consideration could then be given to creating an express exception.

25.162 Use or disclosure for the purpose of legal advice or legal proceedings could be authorised where there is a requisite connection with the primary purpose of collection, and within the reasonable expectations of the individual.[212] The OPC's guidelines in the health area, for example, recognise expressly that disclosure of health information to a lawyer solely for the purpose of addressing liability indemnity arrangements, or for

---

211 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

212 See UPP 5.1(a).

the defence of anticipated or existing legal proceedings, could be directly related secondary purposes.[213]

25.163 The law enforcement exception also expressly authorises use and disclosure of personal information where it is believed to be reasonably necessary by or on behalf of an enforcement body in preparation for, or conduct of, court or tribunal proceedings.[214]

25.164 Lastly, the 'required or authorised by or under law' exception could authorise disclosure of personal information for use in legal proceedings. The ALRC has recommended that the *Privacy Act* should be amended to provide that 'law' for the purposes of determining when an act or practice is required or authorised by or under law includes an order of a court or tribunal.[215] This exception, for example, authorises the disclosure of personal information in legal proceedings pursuant to an order for pre-trial discovery, or a subpoena to produce documents or give evidence.

25.165 In *C v Commonwealth Agency* the Privacy Commissioner formed the view that the disclosure of the complainant's personal information to the legal counsel of the relevant agency was 'authorised by law, as it was subject to legal professional privilege'.[216] The Privacy Commissioner, therefore, held that the exception in NPP 2.1(g)—disclosure authorised by or under law—applied. While the ALRC queries the conclusion that the doctrine of legal professional privilege is capable of authorising a disclosure, the outcome is significant in that it demonstrates the OPC's pragmatic approach in this area.

25.166 The doctrine of legal professional privilege—or client legal privilege, as it is described in the *Evidence Act 1995* (Cth)—in summary, protects from disclosure confidential communications between a lawyer and his or her client made for the dominant purpose of seeking legal advice or for preparing for actual or contemplated litigation. The doctrine of privilege, therefore, has the effect of limiting the interference with the privacy of an individual whose personal information is the subject of protected confidential communications.

25.167 In drafting the model UPPs, the ALRC has assumed that an agency or organisation is entitled to disclose personal information to a legal adviser for the dominant purpose of obtaining legal advice. For example, the 'Collection' principle, UPP 2.4 provides that:

> If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

---

213 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 14–15.

214 See UPP 5.1(f)(v).

215 See Rec 16–1.

216 *C v Commonwealth Agency* [2005] PrivCmrA 3.

> (a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
>
> (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

25.168 As discussed in Chapter 21, an agency or organisation may need to use or disclose personal information in order to receive advice about whether to retain or destroy it.

Logging use and disclosure

25.169 In DP 72, the ALRC considered whether agencies or organisations should be required to record their use or disclosure of personal information when this occurs for a purpose other than the primary purpose of collection. In ALRC 22, the ALRC did not recommend that record-keepers be obliged to keep a log of all uses and disclosures of personal information because the administrative costs would be too high.[217] The ALRC suggested, however, that the Human Rights Commission (as it was then called) should encourage record-keepers to adopt the practice of logging disclosures, at least those disclosures that would represent a particularly objectionable interference with individual privacy.[218]

25.170 Under NPP 2, an organisation is required to make a written note of its use or disclosure of personal information only where it relates to a specified law enforcement purpose.[219] NPP 2 has been criticised on the basis that it does not require organisations to record their use and disclosure of personal information in times of emergencies 'to ensure that a trace of the activities of privacy-abusers is retained'.[220]

25.171 Similarly, IPPs 10 and 11 require an agency to make a written note of its use and disclosure of information only where it is for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue. In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that every agency should keep a record of authorised disclosures of confidential third party information for the purpose of checking the legitimacy of access to such information. It recommended that the record should include the names of individuals and organisations about whom information is

---

217 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [22.114]–[22.117].

218 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Vol 2, 197.

219 See *Privacy Act 1988* (Cth) sch 3, NPP 2.2.

220 R Clarke, 'Serious Flaws in the National Privacy Principles' (1998) 4 *Privacy Law & Policy Reporter* 176, 177.

disclosed, the names of the individuals and organisations to whom that disclosure is made, and the date of the disclosure.[221]

Submissions and consultations

25.172 In response to IP 31, some stakeholders supported a requirement for agencies and organisations to record their use and disclosure of personal information for a secondary purpose.[222] For example, the Australian Privacy Foundation submitted that some record should be kept to allow: reconstruction in the event of an inquiry or challenge; notification of third parties where information is later corrected; and notification of individuals following a security breach.[223]

25.173 A number of stakeholders suggested limitations to the operation of any such requirement. Some stated that it should apply only if there is no direct link between the primary and secondary purpose.[224] The Queensland Government submitted that a more general requirement may result in an 'undue administrative burden'.[225] Other stakeholders submitted that there should be no recording requirement where the individual has consented to the use or disclosure,[226] or where he or she is already aware of the use or disclosure.[227]

25.174 The South Australian Government stated that:

> Importance should be placed on the requirement of agencies and organisations to adhere to records management best practice. In the public sector, governments already have these requirements, supporting the principle that government should be open and accountable to all citizens …
>
> If the exemption for small business is removed then recording use or disclosure could become burdensome. If the regulatory requirements were limited to a high, policy level which addresses systematic practices in which information is used, the regulatory burden would not be as heavy.[228]

---

221 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), rec 6.

222 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; I Turnbull, *Submission PR 82*, 12 January 2007. One stakeholder stated that the obligation should apply to primary and secondary use or disclosure: Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

223 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

224 Queensland Government, *Submission PR 242*, 15 March 2007; Australian Taxation Office, *Submission PR 168*, 15 February 2007; AAMI, *Submission PR 147*, 29 January 2007.

225 Queensland Government, *Submission PR 242*, 15 March 2007.

226 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; AXA, *Submission PR 119*, 15 January 2007.

227 AXA, *Submission PR 119*, 15 January 2007. The OPC submitted that any recording requirement should not impact adversely on the privacy of third parties: Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

228 Government of South Australia, *Submission PR 187*, 12 February 2007.

25.175 The NHMRC stated that such recording represented good practice, but submitted that a 'requirement will impose significant burdens and costs'. It advocated 'an educative approach that highlights the various ways in which information transactions can be recorded and the benefits of doing so where practicable'.[229]

25.176 Some stakeholders were opposed to any such recording requirement. It was submitted that the existing requirements are 'an unmanageable burden' and that any extension would be 'potentially onerous',[230] and would increase the cost of compliance.[231] UNITED Medical Protection stated that such a requirement would place a particular burden on medical practices because considerable time and cost would be required to create the logging system and then to carry out the logging process. It submitted that a better way to protect privacy is through appropriate limitations on use and disclosure.[232]

25.177 The AFP stated that a recording requirement would not 'enhance the current accountability framework applying to police use of personal information' and may lead to duplication.[233]

25.178 In DP 72, the ALRC expressed the preliminary view that it is undesirable to require agencies and organisations to record their use or disclosure of personal information for a purpose other than the primary purpose of collection. The ALRC also expressed the view that the current recording requirements that apply in the law enforcement context should be retained.[234]

25.179 This approach was supported by some stakeholders.[235] The Insurance Council of Australia, for example, strongly opposed a mandatory logging requirement on the basis that 'it would present a major logistical task for little practical benefit'.[236] Other stakeholders stated that the 'Use and Disclosure' principle should incorporate the existing requirements under the IPPs and NPPs relating to logging use and disclosure of personal information for law enforcement purposes.[237] The OPC also suggested that

---

229 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

230 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007.

231 National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.

232 UNITED Medical Protection, *Submission PR 118*, 15 January 2007.

233 Australian Federal Police, *Submission PR 186*, 9 February 2007. See also Law Council of Australia, *Submission PR 177*, 8 February 2007.

234 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [22.114]–[22.117].

235 Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

236 Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

237 Confidential, *Submission PR 570*, 13 February 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

consideration be given to requiring agencies and organisations to keep a log of disclosures under the exception in the 'Use and Disclosure' principle in the model UPPs relating to investigating or reporting unlawful activity.[238]

25.180 The Cyberspace Law and Policy Centre, however, expressed opposition to the suggested approach. It submitted that the 'Use and Disclosure' principle should include a specific requirement to keep a log or record of all uses and disclosures pursuant to each of the exceptions set out in the principle.

> If designed into systems, recording of exceptional uses and disclosures should be both easy and cheap, and would in our view have a wide range of collateral benefits. Good record-keeping is simply good business practice.[239]

ALRC's view

25.181 It is important that agencies and organisations implement proper record-management systems. This is essential for a number of reasons, only one of which is to protect personal information. For example, proper record management is essential in the health care context to facilitate the provision of optimal health care to patients. Similarly, proper record management is critical in criminal investigations to ensure that the continuity of the chain of custody of evidence can be established.

25.182 While the promotion of best practice in record management is to be encouraged, privacy legislation should not mandate that agencies and organisations record each use and disclosure of personal information made for a purpose other than the primary purpose of collection. The sheer volume of use and disclosure of personal information by agencies and organisations on a daily basis would render such a requirement impractical, costly and onerous. This is particularly so for those agencies and organisations that handle large volumes of personal information. Such a requirement cannot be justified on a cost and benefit basis.

25.183 The potential benefits of such an approach include that it would: increase transparency in the handling of personal information by agencies and organisations; and assist individuals in tracing the use and disclosure of their personal information after collection. These benefits are, however, outweighed by the disproportionate compliance burden that would be imposed on agencies and organisations. Moreover, such benefits are likely to be delivered by other mechanisms in the *Privacy Act*, including requirements under the privacy principles relating to notification and openness.[240]

25.184 In addition, the ALRC has recommended that the *Privacy Act* should be amended to impose an obligation on agencies and organisations to notify the Privacy Commissioner and affected individuals about data breaches—essentially unauthorised

---

238 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
239 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
240 See Chs 23 and 24 respectively.

acquisitions of personal information—which may give rise to a real risk of serious harm to individuals.[241] A data breach notification requirement is substantially more likely to deliver increased privacy protection to individuals than a general requirement to log every use and disclosure of personal information for a secondary purpose.

25.185 While imposing a general legislative requirement to log use and disclosure is, on balance, untenable, there is considerable merit in imposing such a requirement in the special context of law enforcement. The existing requirements for agencies and organisations to log uses and disclosures that fall within the relevant law enforcement exception, therefore, should be retained.

Logging reports of unlawful activity

25.186 The ALRC notes that one stakeholder suggested that agencies and organisations should be required to record disclosure of personal information made under the requirement in the 'Use and Disclosure' principle to report suspected unlawful activity to the authorities.

25.187 To the extent that an agency or organisation reports unlawful activity to an enforcement body, it is very likely that such disclosure falls within the parameters of the exceptions relating both to unlawful activity and law enforcement in the 'Use and Disclosure' principle. This is because, in many instances, an agency or organisation would reasonably believe that reporting the information is necessary to allow the enforcement body to investigate the matter. Not all use and disclosure under the unlawful activity exception, however, would overlap with the law enforcement exception. For example, internal use of personal information by an organisation for the purpose of investigating unlawful activity or the reporting of unlawful activity to a relevant person or authority that does not fall within the legislative definition of 'enforcement body' would be outside the scope of the law enforcement exception.

25.188 On balance, given the area of overlap between the exceptions relating to unlawful activity and law enforcement, it seems unnecessary for the *Privacy Act* to require the logging of all use and disclosure under the unlawful activity exception. Such an approach also would increase compliance costs. Moreover, if logging of use and disclosure under the unlawful activity exception were to be mandated, it would create an expectation that logging should be required where personal information is used or disclosed under other, arguably quasi-related, exceptions, such as where use or disclosure is required or authorised by or under law. This would impose potentially disproportionate compliance burdens on agencies and organisations.

241 See Ch 51, Rec 51–1.

Summary of 'Use and Disclosure' principle

25.189 The fifth principle in the model UPPs should be called 'Use and Disclosure'. It may be summarised as follows.

UPP 5. Use and Disclosure

5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) 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;

(b) the individual has consented to the use or disclosure;

(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

(i) an individual's life, health or safety; or

(ii) public health or public safety;

(d) the agency or organisation 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;

(e) the use or disclosure is required or authorised by or under law;

(f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;

(g) the use or disclosure is necessary for research and all of the following conditions are met:

(i) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;

(ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), 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*;

(iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and

(iv) 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; or

(h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.

5.2 If an agency or organisation uses or discloses personal information under paragraph 5.1(f) it must make a written note of the use or disclosure.

5.3 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. Nothing in subclause 5.1 requires an agency or organisation to disclose personal information; an agency or organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: Agencies and organisations also are subject to the requirements of the 'Cross-border Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

26. Direct Marketing

Contents

Introduction

26.1 'Direct marketing' involves the promotion and sale of goods and services directly to consumers. Direct marketing can include both unsolicited direct marketing and direct marketing to existing customers. For unsolicited direct marketing, direct marketers usually compile lists of individuals' names and contact details from many sources, including publicly available sources.[1] An individual may not always know that

1 Such publicly available sources include public registers, for example, state registers of births, deaths and marriages, as well as the internet. Historically, the electoral roll was used for the purpose of direct marketing. Restrictions on the use of the electoral roll for the purposes of direct marketing, however, were introduced by the *Electoral and Referendum Amendment (Access to Electoral Roll and Other Measures) Act 2004* (Cth) sch 1, pt 1, [4]; sch 1 pt 3, [115]. That Act amended the *Commonwealth Electoral Act 1918* (Cth) to extend the end-use restrictions to all roll information. The prohibition on using electoral roll information for commercial purposes applies 'to all roll information, regardless of when it was obtained': J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online

his or her personal information has been collected for the primary purpose of direct marketing. Direct marketing to existing customers may involve communications designed to let customers know about new products or services.

26.2 The *Privacy Act 1988* (Cth) does not define direct marketing. The Office of the Privacy Commissioner's review of the private sector provisions of the *Privacy Act* (the OPC Review) described direct marketing as

> The promotion and sale of goods and services directly to the consumer. Direct marketers promote their goods and services by mail, telephone, email or SMS. They compile lists of consumers and their contact details from a wide variety of sources. These include public records, including the white pages, the electoral roll, registers of births, deaths and marriages and land title registers. They also include membership lists of business, professional and trade organisations, survey returns, mail order purchase and so on.[2]

26.3 The Code of Practice of the Australian Direct Marketing Association (ADMA) defines 'direct marketing' as:

> the marketing of goods or services or the seeking of donations through means of communication at a distance where:
>
> (a) consumers are invited to respond using a means of communication at a distance; and
>
> (b) it is intended that the goods or services be supplied under a contract negotiated through means of communication at a distance.[3]

26.4 This definition has been criticised, however, for failing to reflect the everyday meaning of the term 'direct marketing', because it requires a marketing communication to be at a distance, 'whereas the everyday meaning would include a marketing communication that is not from a distance, such as one that is in person'.[4]

26.5 Direct marketing now represents over 32% of all media spending.[5] ADMA notes that 'direct marketers and their suppliers employ over 660,000 Australians'.[6]

26.6 Direct marketing has been, and continues to be, however, the source of community concern. For example, in a recent survey commissioned by the OPC, 80% of respondents expressed concern or annoyance about receiving unsolicited direct

---

ed, as at 14 March 2008), [98-243]. See also Commonwealth, *Parliamentary Debates*, House of Representatives, 1 April 2004, 27930 (P Slipper).

2 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 94.

3 Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2006), 8.

4 J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online ed, as at 14 March 2008), [25-200].

5 Australian Direct Marketing Association, *Frequently Answered Questions* (2007) <www.adma.com.au/asp/> at 7 April 2008, 1.

6 Ibid.

marketing communications.[7] Such concerns were also reflected in the National Privacy Phone-In conducted by the ALRC on 1 and 2 June 2006, where 73% of calls identified as an issue of concern the receipt of unsolicited communication by way of phone, mail, fax, email and SMS. It is important to note that the community concern expressed in these surveys related to unsolicited direct marketing communications.

26.7 On the other hand, stakeholders made clear that there are pragmatic reasons why those engaged in direct marketing do not wish to communicate with those who do not want to receive direct marketing communications. The Mailing House stated that the industry 'do[es] not wish to irritate the public, abuse the concept of privacy or incur expense on material that has little chance of influencing a response'.[8]

26.8 This chapter first considers whether the privacy principles should regulate direct marketing regardless of whether the personal information in question was collected for a primary or secondary purpose of direct marketing. It then discusses whether direct marketing should be regulated by a separate privacy principle. The chapter also considers whether the *Privacy Act* should regulate direct marketing by agencies. How the 'Direct Marketing' principle in the *Privacy Act* should relate to other legislation that deals with particular forms of direct marketing is considered. The content of the 'Direct Marketing' principle and the need for guidance from the OPC in relation to the 'Direct Marketing' principle is then discussed.

Current coverage by IPPs and NPPs

26.9 The current rules in the *Privacy Act* on direct marketing differ between agencies and organisations. The Information Privacy Principles (IPPs) do not contain any provisions dealing explicitly with direct marketing by agencies. In contrast, the National Privacy Principles (NPPs) deal with the issue of direct marketing by organisations as part of the use and disclosure principle. NPP 2 creates a general prohibition against the use or disclosure of personal information for a secondary purpose, and then lists a number of exceptions to this general rule.[9] The most significant exception is NPP 2.1(c), which permits the use of personal information for the secondary purpose of direct marketing only if all of the following conditions are met:

- the information in question is not 'sensitive information';
- it is impracticable to seek the individual's consent before using the information;

7 Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), 29.
8 The Mailing House, *Submission PR 64*, 1 December 2006.
9 The operation of NPP 2 is considered in greater detail in Ch 25.

- the organisation will not charge the individual for giving effect to a request by the individual not to receive direct marketing communications;

- the individual has not requested the organisation to refrain from providing direct marketing communications;

- in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that the individual may express a wish not to receive any further direct marketing communications; and

- each written direct marketing communication to the individual sets out the organisation's business address and telephone number and, if the communication is made by electronic means, a number or address at which the organisation can be contacted directly electronically.

26.10 Currently, the direct marketing provisions only permit personal information to be used, but not disclosed, for direct marketing.[10] The *Annotated National Privacy Principles* state that, in determining whether it is 'impracticable' to gain consent for the purposes of NPP 2.1(c)(i), relevant factors will include the cost of obtaining consent and any negative privacy implications that may result from not obtaining consent.[11] The factors listed in relation to 'impracticability' in the OPC's *Guidelines to the NPPs* include the consequences for the individual of receiving the information without having consented and how often the organisation is in contact with an individual.[12]

26.11 NPP 2 prohibits an organisation from using or disclosing personal information for the secondary purpose of direct marketing, unless its proposed use or disclosure falls within one of the exceptions in NPP 2.1. In addition to direct marketing permitted by NPP 2.1(c), there are other circumstances in which the use or disclosure of personal information for direct marketing is permitted under the NPPs. These are where

- the individual concerned has consented to its use for that purpose;
- the information was collected for the primary purpose of direct marketing;
- direct marketing is related, or, in the case of sensitive information, 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 direct marketing.[13]

---

10 J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online ed, as at 14 March 2008), [25-320]; Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 38.

11 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2-1125].

12 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 39.

13 J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online ed, as at 14 March 2008), [25-70], referring to *Privacy Act 1988* (Cth) sch 3, NPP 2.1(a), 2.1(b).

26.12 The *Comprehensive Guide to Privacy Law* states that 'if any of these circumstances exist, there is no need to rely on the special direct marketing provisions'.[14] For example, in *E v Motor Vehicle Retail Organisation*,[15] the respondent had collected the complainant's personal information without consent by acquiring a marketing list from another organisation for the purpose of direct marketing. The Privacy Commissioner determined that there was no breach of NPP 2, since the respondent had collected the respondent's personal information for the primary purpose of direct marketing and used it for that purpose.

26.13 It seems that much direct marketing, in particular to existing customers, is facilitated by the other limbs of the use and disclosure principle. For the purposes of NPP 2.1(b), consent can either be express or implied. An example of implied consent for a secondary purpose is where an individual does not 'indicate on an application form that he or she would like to opt-out of receiving direct marketing material where the option to do so is clearly indicated above the signature box'.[16]

Issues in current coverage by the NPPs of direct marketing

26.14 Issues arising from the practice of direct marketing and the application of the principles dealing with direct marketing were considered by the OPC Review.[17] These included, for example, whether the *Privacy Act* should contain the assumption that personal information may be used for direct marketing. The OPC recommended that the Australian Government should consider:

- amending the *Privacy Act* to provide consumers with a general right to opt out of direct marketing approaches at any time and to require that organisations comply with such a request within a specified time;[18]

- amending the *Privacy Act* to require organisations to take reasonable steps, on request, to advise an individual where it acquired the individual's personal information;[19] and

- exploring options for establishing a national 'Do Not Contact' register.[20]

26.15 In response to the Issues Paper, *Review of Privacy* (IP 31), the Law Council of Australia submitted that there should be a separate privacy principle dealing with direct

---

14 J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online ed, as at 14 March 2008), [25-60].

15 *E v Motor Vehicle Retail Organisation* [2004] PrivCmrA 19; cited in J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2-906].

16 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2-1040].

17 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 94–103.

18 Ibid, rec 23, 11, 103.

19 Ibid, rec 24, 11, 103.

20 Ibid, rec 25, 11, 103.

marketing, and that it should apply regardless of whether the relevant personal information was collected for the primary purpose or a secondary purpose of direct marketing.[21] This is because the current provisions permit personal information that is collected for the primary purpose of direct marketing to be used 'almost without restraint'.[22] The Law Council submitted that:

> There appears to be no valid policy reason why an organisation which collects information for the primary purpose of direct marketing should be free to use that information in a way which organisations which collect it in the context of a relationship with the individual are not free to use it. Indeed, from a policy perspective you might expect fewer, not more, constraints on an organisation with which an individual has chosen to deal as opposed to an organisation which has no relationship with an individual but buys their information for the purpose of marketing to them.[23]

26.16 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC noted that there is currently considerable ambiguity about whether organisations have collected personal information for the primary or secondary purpose of direct marketing. There also may be some deliberate or unintended obfuscation. For example, where individuals are asked to provide personal information to make them eligible to win a prize, the individuals might assume that the primary purpose of the collection is to make them eligible for the prize, whereas the primary purpose of the organisation collecting this information may in fact be to create a database from which to carry out direct marketing. The OPC Review observed that 'even if the individual reads the fine print, he or she is unlikely to draw a distinction between a primary and secondary purpose and to understand the consequences of the decision'.[24] This problem would be eliminated by making the direct marketing rules apply regardless of whether the personal information in question was collected for the primary purpose of direct marketing or whether it was a secondary purpose.

26.17 In DP 72, the ALRC expressed the preliminary view that stakeholder concerns regarding the direct marketing activities of some organisations are unlikely to be addressed adequately if the relevant privacy principle only covers secondary purpose direct marketing. Consequently, the ALRC proposed that the *Privacy Act* should apply to direct marketing, whether the individual's personal information was collected for the primary purpose *or* a secondary purpose of direct marketing.

26.18 In DP 72, the ALRC stated that, if this reform is adopted, the rationale for locating the direct marketing provisions in the general use and disclosure privacy principle would be severely undermined. Moreover, given that direct marketing is relevant to other aspects of the information cycle—most notably, the collection of

---

21 Law Council of Australia, *Submission PR 177*, 8 February 2007.

22 Ibid. See also Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144*, 25 January 2007.

23 Law Council of Australia, *Submission PR 177*, 8 February 2007.

24 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 95.

personal information and the maintenance of data quality and data security—the ALRC noted that it is logical to create a discrete privacy principle to regulate direct marketing. The ALRC proposed that the Unified Privacy Principles (UPPs) should regulate direct marketing by organisations in a discrete privacy principle, separate from the 'Use and Disclosure' privacy principle, to be called 'Direct Marketing'.[25]

Submissions and consultations

26.19 The proposal was supported by a large number of stakeholders.[26] The Public Interest Advocacy Centre (PIAC) supported the removal of the distinction between primary and secondary purpose direct marketing:

> In many cases it will be too difficult to determine whether direct marketing is a primary or a secondary purpose of collection. The proposed UPP will avoid the need to get bogged down in this type of argument.[27]

26.20 The OPC submitted that the proposed separate principle was 'an appropriate response to the demonstrable community concern regarding the handling of personal information for direct marketing'.[28] GE Money Australia submitted that the proposed principle would assist in 'providing clarity' as to the rules associated with direct marketing for organisations engaged in it.[29] The Insurance Council of Australia submitted:

> It is anomalous that those who intend to use personal information for direct marketing as a secondary purpose currently have significantly more onerous obligations than those who receive consent for direct marketing as a primary purpose.[30]

26.21 A number of stakeholders, however, did not support a separate principle.[31] Optus submitted that direct marketing

> serves an important economic function and is a vital component of Australian business … Many Australians purchase goods and services through direct marketing channels. Further, the ability to use customer information for the secondary purpose of direct marketing prevents anonymous direct marketing contacts and allows more

---

25 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 23-1.

26 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; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Obesity Policy Coalition, *Submission PR 506*, 20 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; ANZ, *Submission PR 467*, 13 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

27 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

29 GE Money Australia, *Submission PR 537*, 21 December 2007.

30 Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

31 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

> targeted direct marketing. More targeted direct marketing results in direct marketing approaches being made to parties that are interested in receiving an approach by an organisation. There are two significant positive effects that arise from targeted marketing. Firstly it reduces the number of unwanted direct marketing contacts. Secondly it increases business efficiency.[32]

26.22 The Australian Bankers' Association (ABA) submitted that direct marketing was simply one aspect of use and disclosure.[33] Acxiom submitted that privacy legislation was not 'the appropriate mechanism through which to regulate specific industry sectors or industry practices'.[34] ADMA and Acxiom argued that it was more appropriate for the UPPs to remain both technologically neutral and non-industry or practice specific.[35] They submitted that more detailed rules relating to direct marketing should be addressed by a registered industry code of practice or in guidance published by the OPC.[36]

26.23 The Law Council of Australia submitted:

> The impact of the proposed change is the direct marketers would always be required to obtain consent (where it is practical to do so) and to provide an opt-out to recipients, even where the information was collected for the primary purpose of direct marketing and where there is an existing business relationship (although arguably this may give rise to an implied consent).[37]

26.24 Some stakeholders took issue with the description of direct marketing in DP 72.[38] ADMA argued that the 'definition' of direct marketing focused on 'unsolicited communications' and did not capture 'direct marketing to individuals with whom organisations have existing business relationships'.[39] ADMA argued that 'direct marketers do not "compile lists" of current customers from external sources because they have already been given the data'.[40] ADMA also pointed out that 'legislation ensures that the electoral roll is not to be used for direct marketing purposes and telephone directories are protected by copyright'.[41]

---

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

33 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008. Also: Acxiom Australia, *Submission PR 551*, 1 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007.

34 Acxiom Australia, *Submission PR 551*, 1 January 2008.

35 Ibid; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

36 Acxiom Australia, *Submission PR 551*, 1 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

37 Law Council of Australia, *Submission PR 527*, 21 December 2007.

38 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [23.1].

39 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

40 Ibid.

41 Ibid. See also Acxiom Australia, *Submission PR 551*, 1 January 2008.

26.25 Some stakeholders called for the term 'direct marketing' to be defined.[42] For example, the Cyberspace Law and Policy Centre and the Australian Privacy Foundation suggested the *Privacy Act* should define direct marketing as

> the marketing or promotion of goods, services or ideas, including fundraising and recruitment, by direct targeted communication with specific individuals or by individualized communications by any means.[43]

26.26 The Law Council called for the definition of direct marketing in the OPC Review, referred to above, to be adopted.[44] A number of stakeholders also called for a distinction to be made between direct marketing to existing customers and direct marketing to prospective customers.[45] ADMA submitted:

> It is vital to make the distinction between direct marketing to existing customers and unsolicited direct marketing to prospective customers.
>
> Marketing to existing customers is both a legitimate business activity and essential as it ensures that an organisation can meet the needs of its customers by offering the most appropriate and cost effective products and services to consumers that it has already established a relationship with.[46]

ALRC's view

26.27 The issue of direct marketing has been, and continues to be, the subject of a very strong response from stakeholders and the community generally. On one hand, there is a strong push from consumers and consumer advocates to tighten the rules on direct marketing to make it more difficult for companies engaged in direct marketing to communicate with people in this way, particularly with respect to unsolicited direct marketing. This draws on the conceptualisation of privacy as including, at least, 'the right to be let alone'.[47]

26.28 On the other hand, business groups and others have emphasised the importance of direct marketing for the economy generally. They have also stressed that, if direct marketing is carried out appropriately, it can be of considerable assistance to consumers that receive direct marketing communications.

26.29 It is possible to balance these competing positions by recognising both that some forms of direct marketing can be pernicious and can erode individuals' privacy rights but that, if undertaken appropriately, direct marketing also can be beneficial.

---

42 Law Council of Australia, *Submission PR 527*, 21 December 2007.

43 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

44 Law Council of Australia, *Submission PR 527*, 21 December 2007.

45 Acxiom Australia, *Submission PR 551*, 1 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007.

46 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

47 See S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 193. Note, however, that the definition of the 'right to privacy' should not be reduced only to the right to be left undisturbed. As explained in Ch 1, the modern conceptualisation of privacy involves many other elements.

26.30 The *Privacy Act* currently deals with the issue of direct marketing by organisations as part of the use and disclosure principle in NPP 2. There currently is considerable ambiguity as to whether organisations, which collect personal information that they later intend to use for direct marketing, have collected this information for the secondary purpose of direct marketing. The concerns expressed by stakeholders regarding the direct marketing activities of some organisations are unlikely to be addressed adequately if the relevant privacy principle only covers secondary purpose direct marketing.

26.31 The model UPPs should regulate direct marketing by organisations in a discrete privacy principle, which should apply regardless of whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing.

26.32 The ALRC acknowledges the issues raised by stakeholders about the description of direct marketing in DP 72, and has attempted to address those concerns in this chapter. The ALRC notes, however, that while some stakeholders called for the term 'direct marketing' to be defined for the purposes of the *Privacy Act*, there is no consensus about how that term should be defined. In the ALRC's view, the scope of the term generally seems to be understood. Concerns raised in relation to direct marketing were not definitional—instead the concerns raised were about the process of direct marketing, in particular, unsolicited direct marketing. To define direct marketing may unnecessarily confine the application of the 'Direct Marketing' principle. For example, if direct marketing is defined by reference to current practice, but practice later evolves, new methods of direct marketing may not be caught by the definition and so would not be subject to the 'Direct Marketing' principle. In the ALRC's view, 'direct marketing' should not be defined for the purposes of the Act.

26.33 The requirements that apply to direct marketing communications to individuals who are not existing customers should be more onerous than those applying in the context of direct marketing to existing customers. The reasons for this distinction are discussed later in relation to the content of the model 'Direct Marketing' principle.

Recommendation 26–1 The model Unified Privacy Principles should regulate direct marketing by organisations in a discrete privacy principle, separate from the 'Use and Disclosure' principle. This principle should be called 'Direct Marketing' and it should apply regardless of whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing. The principle should distinguish between direct marketing to individuals who are existing customers and direct marketing to individuals who are not existing customers.

Application of direct marketing principle to agencies

26.34 Before considering the content of the direct marketing principle, first it is necessary to consider what entities should be bound by the principle. Currently, organisations must comply with the direct marketing provisions in NPP 2.1(c) where direct marketing does not fall within one of the other limbs of the use and disclosure principle in NPP 2. On the other hand, agencies are not subject to any express regulation of direct marketing in the IPPs.

26.35 The OPC's guidelines on the IPPs state that 'agencies' are generally federal government organisations, but notes that some types of organisations, 'even if set up by federal government laws', are not agencies.[48] For example, incorporated companies are excluded from the definition of 'agency' in the *Privacy Act.*[49] Also, the term 'organisation' is defined to exclude an 'agency'.[50] Acts of certain prescribed agencies, however, may be treated as acts of organisations.[51]

> The Government's policy is that bodies operating in the commercial sphere should operate on a level playing field. Where agencies are engaged in commercial activities, they should be required to comply with the NPPs, just like private sector organisations. [52]

26.36 The *Privacy (Private Sector) Regulations 2001* (Cth) prescribe the Australian Government Solicitor and the Australian Industry Development Corporation as agencies to be treated as organisations under the *Privacy Act*.[53]

26.37 State and territory authorities fall outside the definition of 'agency' and are expressly excluded from the definition of 'organisation' under the *Privacy Act*.[54] However, they can be brought into the regime by regulation. A number of state authorities have been prescribed as organisations for the purposes of the *Privacy Act,* including, for example, Energy Australia and Integral Energy.[55]

26.38 State instrumentalities are treated as organisations under the *Privacy Act* unless they have been prescribed to fall outside of the definition of 'organisation' under s 6C(4) of the *Privacy Act.*[56] On the other hand, state and territory statutory

---

48 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 4.

49 *Privacy Act 1988* (Cth) s 6(1).

50 Ibid s 6C(1). State and Territory instrumentalities will be caught by the definition of 'organisation' unless they are prescribed in regulations under s 6C(4) of the *Privacy Act*, which allows for regulations to be made to stop state or territory instrumentalities from being organisations for the purposes of the Privacy Act: Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [74].

51 *Privacy Act 1988* (Cth) s 7A.

52 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [102].

53 *Privacy Act 1988* (Cth) s 7A; *Privacy (Private Sector) Regulations 2001* (Cth) cl 4.

54 *Privacy Act 1988* (Cth) ss 6(1), 6C.

55 Ibid s 6F; *Privacy (Private Sector) Regulations 2001* (Cth) cl 3A.

56 *Privacy Act 1988* (Cth) s 6F. See discussion in Ch 38.

corporations are excluded from the coverage of the *Privacy Act*.[57] The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 noted that state and territory statutory corporations would not be caught by the definition of 'organisation', but that 'Government Business Enterprises that are Corporations Law corporations' would fall within the definition.[58] The latter therefore would be subject to the model 'Direct Marketing' principle in the same way as other organisations. The extent to which state and territory state-owned corporations, statutory corporations and government business enterprises should be regulated by the *Privacy Act* is discussed in Chapter 38.

26.39 Also relevant in this context is s 16F of the *Privacy Act*, which provides that personal information collected under a Commonwealth contract is not to be used or disclosed for direct marketing.

26.40 It appears that, currently, the *Privacy Act* is structured so that government business enterprises which operate in competition with private sector organisations generally will not be considered agencies for the purposes of the *Privacy Act*. In the context of other statutory regimes, however, the Government has expressed the policy position that, even if legislation technically does not apply to government bodies who are in competition with the private sector, it will be best practice for such government bodies to meet legislative requirements in relation to those commercial activities. For example, guidance published for government bodies on the *Spam Act 2003* (Cth) considers the application of that legislation in circumstances where a government body may be commercialised or operating in a competitive environment. It states:

> In these circumstances it is important that government is not perceived as having undue advantage. It is strongly recommended that you do not rely on the exemptions that apply to government bodies when sending commercial electronic messages. You should aim for best practice by ensuring you fully meet, or exceed, the requirements of the *Spam Act*.[59]

26.41 In DP 72, the ALRC asked whether agencies should be subject to the proposed 'Direct Marketing' principle and, if so, whether any exceptions or exemptions should apply specifically to agencies.[60]

---

57 Ibid s 6C(3).

58 The term 'State or Territory authority' is also defined to exclude 'an incorporated company, society or association'. The Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [73] states that state or territory authorities are, in general terms, defined to mean people or bodies that are part of the state or territory public sector. Local councils will generally fall within the definition of 'State or Territory authority'. Government business enterprises may be excluded from the coverage of the *Privacy Act* if they are prescribed under s 6C(4).

59 Australian Communications Authority, *Spam Act 2003: A Practical Guide for Government*, 1 April 2004, 13.

60 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 23–1.

Submissions and consultations

26.42 There was some support for the application of the principle to agencies.[61] The Law Council of Australia submitted that it was consistent with the proposal for one unified set of principles.[62] In a similar vein, PIAC submitted:

> There has been an increasing tendency for government agencies to use direct marketing techniques to promote government services and programs. Extension of the direct marketing principle to cover agencies would also be consistent with Proposal 15–2 (the development of a single set of privacy principles applicable to both the public and the private sector). There should be exceptions in circumstances where government agencies have a legitimate reason for communicating information to individuals, eg public health and safety campaigns.[63]

26.43 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre argued that 'the boundaries between private and public sectors are increasingly blurred, and government agencies are now commonly undertaking direct marketing activities'.[64] The Cyberspace Law and Policy Centre noted that the equivalent principle in the Hong Kong *Personal Data (Privacy) Ordinance*[65] applies to all sectors and that the Hong Kong Privacy Commissioner has found public sector bodies in breach of it.[66]

26.44 Agencies submitted, however, that there is a legitimate distinction to be drawn between the direct marketing activities of organisations and those of agencies.[67] For example, Medicare submitted that the 'Direct Marketing' principle should not apply to agencies and stated that:

> Government agencies would only be contacting individuals to offer and/or promote government services, as opposed to private sector enterprises who are trying to sell goods for their own commercial benefit. Government services are offered on the basis that they are of benefit to the public.[68]

26.45 The Australian Taxation Office (ATO) commented that it uses SMS as a means of reminding individuals about upcoming lodgement obligations and publications such as Activity Statement Updates to assist taxpayers to complete their Business Activity Statement correctly.[69] The ATO submitted that they did not see such activity as direct

---

61 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 535*, 21 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

62 Law Council of Australia, *Submission PR 527*, 21 December 2007.

63 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

64 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

65 *Personal Data (Privacy) Ordinance* (Hong Kong).

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

67 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

68 Medicare Australia, *Submission PR 534*, 21 December 2007.

69 Australian Taxation Office, *Submission PR 515*, 21 December 2007.

marketing and presumed that any 'Direct Marketing' principle would not apply to this kind of client contact.[70] The Department of Agriculture, Fisheries and Forestry submitted:

> Agencies operate in the public interest, not their own commercial interests. This suggests different considerations should apply. Public-interest based marketing (eg a quarantine campaign) might be nullified or made largely ineffective if similar principles applied.[71]

26.46 This view was shared by the OPC, who submitted that the 'Direct Marketing' principle should not apply to agencies. While noting that it supported the minimisation of exceptions to the *Privacy Act*, the OPC recognised that it is a 'legitimate function' of agencies to ensure individuals are 'kept informed of policies, services and entitlements relevant to them'.

> Permitting individuals to opt-out of receiving this type of information from agencies may lessen the extent to which the community is aware of what the government is doing and what effect it may have on individuals.
>
> Communications campaigns conducted by agencies are qualitatively different to the practice of 'Direct Marketing' in the private sector, in that they are not conducted primarily to generate a benefit or advantage to the entity, but rather to promote a fully informed constituency.[72]

26.47 The OPC acknowledged that 'agencies do not have, and should not have, an unfettered right to use personal information to contact individuals for any purpose unrelated to their administrative and policy responsibilities', but argued that this would be regulated by the 'Use and Disclosure' principle of the model UPPs.[73]

ALRC's view

26.48 If the 'Direct Marketing' principle, in the form recommended by the ALRC, is made applicable to agencies, this could have a significant impact on the way in which government agencies communicate with individuals. In reaching this view, the ALRC understands that 'agency' will not generally include Commonwealth, state or territory commercial enterprises which are in competition with private sector organisations. The extent to which state and territory state-owned corporations, statutory corporations and government business enterprises should be regulated by the *Privacy Act* is considered in Chapter 38.[74] To the extent that any government body is engaged in commercial activities, it should adopt best practice by ensuring it meets the requirements applying to organisations under the 'Direct Marketing' principle. If the 'Direct Marketing' principle applied to agencies, it may preclude the legitimate communication of

---

70 Ibid.
71 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.
72 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
73 Ibid.
74 See Recs 38–2, 38–3.

important information by agencies. The 'Direct Marketing' principle should not, therefore, apply to agencies.

Relationship between privacy principles and other legislation

Background

26.49 This part of the chapter considers how the 'Direct Marketing' principle should relate to sectoral legislation that deals with particular types or aspects of direct marketing. For example, some aspects of telemarketing are regulated by the *Do Not Call Register Act 2006* (Cth) and some aspects of email marketing are covered by the *Spam Act*. This raises the question whether the regulation of direct marketing should be dealt with by a 'one size fits all' model in the privacy principles, or by sectoral legislation tailored to particular types of direct marketing, or a combination of both.

26.50 In DP 72, the ALRC discussed three main options for reform. First, the UPPs could refrain from dealing with direct marketing, given that it is being regulated elsewhere. Secondly, the sectoral legislation that deals with specific types of direct marketing could be repealed, with the UPPs providing the sole form of regulation in respect of all forms of direct marketing. Thirdly, the UPPs could regulate direct marketing, except to the extent that more specific sectoral legislation covers a particular aspect or type of direct marketing. The sectoral legislation could either provide more or less stringent privacy protection.

26.51 The ALRC proposed that the 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.[75]

Submissions and consultations

26.52 A number of stakeholders supported the proposal.[76] For example, the Department of Broadband, Communications and the Digital Economy (DBCDE) submitted:

> During the development of the *Spam Act 2003* (which regulates electronic messages) and the *Do Not Call Register Act 2006* (which regulates phone calls), the Department received a number of approaches from individuals and small business calling for additional controls on other forms of direct marketing. The proposed UPP 6 would appear to respond to these concerns … [77]

---

75 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 23–2.

76 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

77 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

26.53 The Australian Communications and Media Authority (ACMA) supported the proposal and agreed that imposing a blanket rule for all types and aspects of direct marketing would be too rigid. It submitted that specific legislation such as the *Do Not Call Register Act* can be developed 'that is more responsive to the specific needs of consumers and business'.[78]

26.54 Some stakeholders, such as the Consumer Action Law Centre, argued that the current sector-specific legislation can be enhanced.[79] The Australian Privacy Foundation and the Cyberspace Law and Policy Centre were supportive of the ALRC's proposal but argued that any sectoral legislation as far as possible should be consistent with the 'Direct Marketing' principle, and that any weakening of standards should be justified.[80] PIAC's support was conditional on sectoral legislation imposing more stringent requirements on direct marketing than the standards in the *Privacy Act*.[81]

26.55 The OPC submitted that the 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing.[82] It noted that the enactment of future legislation to regulate sector-specific direct marketing was a matter for Parliament and did not need to be anticipated expressly in the 'Direct Marketing' principle.[83]

26.56 Some stakeholders argued that there should be appropriate consultation with the OPC and other relevant bodies before specific sectoral legislation is enacted, in order to ensure, from a compliance perspective, appropriate alignment with the *Privacy Act*.[84]

26.57 BPay expressed support for displacing the 'Direct Marketing' principle where there is more specific sectoral legislation. It argued, however, that wherever possible, legislation should be in the *Privacy Act* since 'reducing overlap with the *Privacy Act* is likely to minimise confusion and unnecessary duplication of compliance activities for organisations'.[85]

26.58 A number of other stakeholders expressed qualified support. The principal reason for reservations was a concern about the need for certainty as to the regime applying to any particular form of direct marketing.[86] The Law Council of Australia identified the risk of confusion if it is not made clear whether sectoral legislation

---

78 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.
79 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.
80 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
81 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
82 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
83 Ibid.
84 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.
85 BPay, *Submission PR 566*, 31 January 2008.
86 See, eg, GE Money Australia, *Submission PR 537*, 21 December 2007.

displaces the principles. It called for any sectoral legislation that displaces the 'Direct Marketing' principle to be 'specifically referred to in Guidelines to the Principle'.[87]

26.59 Microsoft Asia Pacific submitted that the 'existing regulatory overlaps' were 'inefficient and costly for both regulated entities and the government' and gave rise to uncertainty. Microsoft also expressed concern about existing inconsistencies between the *Privacy Act* and sectoral direct marketing legislation; and state and territory legislation, such as the *Fair Trading Act 1987* (NSW), which it argued regulates the same conduct. Microsoft submitted that these legislative regimes should be harmonised where possible. It expressed a preference for regulation of direct marketing to be consolidated at the federal level, or if that is not possible for constitutional reasons, a Commonwealth-State cooperative scheme.[88]

26.60 Other stakeholders strongly disagreed with the ALRC's proposal.[89] ADMA argued that organisations that undertake direct marketing are currently subject to differing obligations 'depending on the channel through which the marketing is being sent', citing the *Spam Act* and the *Do Not Call Register Act* as examples.[90] ADMA's strong view was that all industry sectors, including the public sector, should be subject to the same legislative requirements with respect to the use of personal information for direct marketing purposes, and that the UPPs should override any specific sectoral legislation regulating a particular type or aspect of direct marketing.[91]

ALRC's view

26.61 The 'Direct Marketing' principle should set out general requirements with respect to direct marketing, but these requirements should be able to be displaced by more specific legislation that deals with a particular type of direct marketing, or direct marketing by a particular technology.

26.62 Making clear that the 'Direct Marketing' principle in the *Privacy Act* sets out the general requirements in this area, and that these may be displaced by other requirements in certain contexts, where Parliament deems it appropriate, allows for a regime that is more responsive to the specific needs of consumers and business.

26.63 This approach is preferable to the other options for regulating direct marketing. Imposing a blanket rule for all forms of direct marketing is too rigid. For example, there is a strong community view that some forms of direct marketing are, or have the capacity to be, more intrusive than others. Clearly, those forms of direct marketing should be subject to regulation that differs from the rules applicable to less intrusive forms of direct marketing. Indeed, this explains the advent of sectoral legislation such

---

87 Law Council of Australia, *Submission PR 527*, 21 December 2007.
88 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.
89 Acxiom Australia, *Submission PR 551*, 1 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007.
90 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.
91 Ibid. See also Acxiom Australia, *Submission PR 551*, 1 January 2008.

as the *Do Not Call Register Act* and the *Spam Act*. Similarly, relying on such sectoral legislation to the exclusion of the *Privacy Act* is problematic, because it leaves loopholes that could encourage other types of direct marketing that also may be intrusive.

26.64 The ALRC's preferred approach allows, for example, the 'Direct Marketing' principle in the *Privacy Act* to operate alongside the more specific provisions in the *Do Not Call Register Act* and the *Spam Act*. The ALRC notes that, currently, a number of exemptions apply in the context of the *Do Not Call Register Act* and the *Spam Act*—for example, charities and religious organisations are excluded.[92] These exemptions may not apply under the *Privacy Act*.

26.65 Finally, the requirements of the 'Direct Marketing' principle should not be able to be displaced only by *more* onerous requirements in sectoral legislation. While such an approach may be appealing to those opposed to direct marketing, it would limit Parliament's options when considering whether to pass sectoral legislation dealing with specific aspects of direct marketing. This, in turn, would ultimately undermine the responsiveness of the regime to the specific needs of those affected by a particular aspect or type of direct marketing.

Recommendation 26–2 The 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.

Content of the 'Direct Marketing' principle

26.66 This part of this chapter considers the content of the 'Direct Marketing' principle. First, the distinction between existing customers and prospective customers is considered. Secondly, the 'opt-out' model is discussed. The extent to which specific provision should be made for children and young people in the 'Direct Marketing' principle is then addressed, and the timeframes for compliance with requests to opt out of direct marketing are considered. Finally, the issue of whether there should be an obligation on organisations involved in direct marketing to disclose the source of personal information is discussed.

Existing customers

26.67 As discussed above, the ALRC recommends that the 'Direct Marketing' principle should distinguish between direct marketing to individuals who are 'existing

92 *Spam Act 2003* (Cth) s 4; sch 1, cl 3; *Do Not Call Register Act 2006* (Cth) s 4; sch 1, cl 2.

customers' and direct marketing to individuals who are not 'existing customers'.[93] This distinction addresses the concerns raised by stakeholders that direct marketing to existing customers is a legitimate business activity and is acceptable where it is within the reasonable expectations of such customers. The framework now recommended by the ALRC was developed in response to issues identified by stakeholders in DP 72.

26.68 It is necessary to consider the appropriate scope of the concept of an 'existing customer'. A number of regimes rely on the notion of an ongoing commercial or business relationship. ADMA's *Direct Marketing Code of Practice*, for example, defines 'unsolicited' to mean:

> a communication sent to a recipient: (a) with whom the message originator does not have an ongoing commercial or contractual relationship; or (b) that has not consented to the receipt of such communications.[94]

26.69 The OPC's submission to the Senate Legal and Constitutional Legislation Committee Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000 discussed the extent to which an opportunity to 'opt out' should be provided. In doing so, the OPC commented:

> The need to provide a chance to opt-out for each use for direct marketing might need to be qualified so that it applies except where the use is clearly within the reasonable expectations of the individual concerned, or is consistent with an ongoing business relationship between the individual concerned and the direct marketer.[95]

26.70 Further, both the *Spam Act* and the *Do Not Call Register Act* currently draw on the concept of existing 'business and other relationships' in defining consent. For the purposes of the *Spam Act* and the *Do Not Call Register Act*, consent is defined to include 'consent that can reasonably be inferred from (i) the conduct; and (ii) the business and other relationships; of the individual and organisation concerned'.[96] In the context of the Do Not Call Register scheme, guidance published by ACMA states:

> In the absence of express consent to receiving telemarketing calls, consent may still be able to be reasonably inferred from both an individual's conduct and their business or other relationships. For example, it is possible that a person who holds a 'XYZ Bank' credit card may reasonably expect to receive calls about 'XYZ Bank' home loans or 'XYZ Bank' savings products.
>
> However, it is less likely to be reasonable for a person with a 'XYZ Bank' credit card to be cold called by 'Lucky's Financial Services', regardless of the subsidiary relationship these entities share.[97]

---

93 Rec 26–1.

94 Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2006), 9.

95 Office of the Federal Privacy Commissioner, *Submission to the Senate Legal and Constitutional Legislation Committee Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 1 September 2000, 10.

96 *Spam Act 2003* (Cth) sch 2, cl 2; *Do Not Call Register Act 2006* (Cth) sch 2, cl 2.

97 Australian Communications and Media Authority, *Do Not Call Register—A Guide for Your Business* (2007), 4.

26.71 ACMA's guidance on the *Spam Act* also considers the concept of a 'pre-existing relationship':

> Consent will not always be inferred where there is a pre-existing relationship. Transactions such as the purchase of a publication or service, attendance at a function, conference or performance alone are unlikely to be a sound basis for inferring consent or assuming that there is a pre-existing relationship.[98]

26.72 Another ACMA publication, addressing consent in the context of the Do Not Call Register scheme, states that it is necessary to look at consent on a 'case-by-case basis, and assess what sort of telemarketing calls a person would reasonably expect to receive under the inferred consent provisions'.[99]

26.73 The concept of 'reasonable expectations' already exists in the *Privacy Act*. As discussed above, one of the circumstances in which direct marketing is permitted under NPP 2 is where direct marketing is related to the primary purpose of collection (or in the case of sensitive information, is directly related to that primary purpose) and the individual concerned would reasonably expect the organisation to use or disclose the information for direct marketing.[100]

26.74 Factors to consider in order to determine whether a use or disclosure of personal information for a secondary purpose is within an individual's reasonable expectations for the purposes of NPP 2.1(a)(ii) include, for example:

- whether the individual knew, or it was clear from the circumstances surrounding the collection, that the information may be used for the secondary purpose;
- whether a high level of confidentiality or sensitivity attaches to the information;
- whether it is common business practice to use or disclose the information for the secondary purpose; and
- whether the organisation is under a duty of care or bound by a professional code of conduct or professional standards of which the individual would reasonably be aware and which would require the organisation to make the secondary use or disclosure.[101]

26.75 Further, as discussed above, both the *Spam Act* and the *Do Not Call Register Act* utilise the concept of 'reasonable expectations'.

---

98 Australian Communications Authority, *Spam Act 2003: A Practical Guide for Government*, 1 April 2004, 6.

99 Australian Communications and Media Authority, *Do Not Call Register—Consent: Information for Industry* (2007), 2.

100 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(a).

101 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2-995].

26.76 The concept of 'impracticability' is already used in the context of secondary purpose direct marketing in NPP 2.1(c)(i). The Macquarie Dictionary defines 'impracticable' as 'not practicable; that cannot be put into practice with the available means'.[102] The *Comprehensive Guide to Privacy Law* states that the requirement of impracticability in NPP 2.1(c) is 'likely to apply only in a minority of cases as, in the majority of cases, it will be practicable to seek consent'.[103] In other contexts in which the concept of 'impracticability' is operative under the *Privacy Act*, such as the research context, factors such as the quantity, age or accessibility of the records are relevant to a determination of whether it is impracticable to obtain consent.[104]

Submissions and consultations

26.77 In ADMA's view, disclosure and use of personal information for direct marketing purposes is within an existing customer's 'reasonable expectations'.[105] ADMA submitted that the ALRC should adopt a definition of 'direct marketing' that either discerns between current and prospective customers or otherwise preserves the ability of organisations to direct market to existing customers, subject to their 'reasonable expectations'.[106] In a similar vein, Acxiom submitted:

> Direct marketing involves both solicited and unsolicited marketing and, as the *Privacy Act* applies to both, the provisions contained within must not be so draconian as to inadvertently over regulate solicited communications as a by-product of attempting to control unsolicited communications. [107]

26.78 Similarly, Optus 'strenuously' objected to the 'imposition of obligations under the current NPP 2.1(c) to both prospective and customer data', because to do so would involve significant costs to business.[108]

26.79 The Law Council of Australia criticised the 'Direct Marketing' principle proposed in DP 72 on the basis that its impact would be always to require consent even where there was an existing business relationship, unless it could be argued that such a relationship gave rise to an implied consent. It also commented:

> Organisations will need complete clarity on when this principle will apply and in particular whether it will apply:
>
> (a) to marketing activities to existing customers; and
>
> (b) if so, whether it is only intended to address marketing to those existing customers a product or service they do not currently have, or whether it could

---

102 *Macquarie Dictionary* (online ed, 2007).

103 J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online ed, as at 14 March 2008), [25-330].

104 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)]. This concept of impracticability in the research context is discussed in detail in Ch 65.

105 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

106 Ibid.

107 Acxiom Australia, *Submission PR 551*, 1 January 2008.

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

> capture activity designed to promote the use of, or the purchase of supplementary goods and services (for example accessories) for use with, a product or service the customer already holds.[109]

26.80 One stakeholder raised concerns about a blanket prohibition against using sensitive information for the purposes of direct marketing, arguing that restricting the use of health information in this way may not be in best interests of consumers. For example, the Broader Health Cover initiative under the *Private Health Insurance Act 2007* (Cth) allows a private health insurer to offer chronic disease management and preventative health programs to members. It was argued, however, that such offers have to be targeted to the health needs of particular individuals and can be made safely only by direct marketing communications.[110]

ALRC's view

26.81 As stated above, the ALRC recommends that the requirements that apply to direct marketing communications to individuals who are not existing customers should be more onerous than those applying in the context of direct marketing to existing customers.

26.82 In relation to existing customers, the ALRC recommends that an organisation may use or disclose personal information about an individual who is an existing customer for the purposes of direct marketing only where the individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing.

26.83 While sensitive information cannot be used for the secondary purpose of direct marketing under NPP 2.1(c), there are some circumstances in which sensitive information can be used for the primary purpose of direct marketing under the NPPs.[111] The model 'Direct Marketing' principle recommended by the ALRC allows sensitive information to be used or disclosed for the purpose of direct marketing to existing customers only where it is within the customer's reasonable expectations. As noted above, one of the factors in determining whether a use or disclosure is within the reasonable expectations of an individual is whether a high level of sensitivity attaches to the information.[112] Submissions also illustrated that there may be circumstances in which such direct marketing would serve the interests of an existing customer. It is

---

109 Law Council of Australia, *Submission PR 527*, 21 December 2007.

110 Confidential, *Submission PR 519*, 21 December 2007.

111 Currently, under the NPPs, sensitive information can be used or disclosed for the primary purpose of direct marketing if the individual consents; if the sensitive information was collected for the primary purpose of direct marketing; or if the direct marketing is directly related to the primary purpose of collection of the sensitive information and the individual concerned would reasonably expect the organisation to use or disclose the sensitive information for the purposes of direct marketing: *Privacy Act 1988* (Cth) sch 3, NPP 2.1(a), 2.1(b). See J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online ed, as at 14 March 2008), [25-70].

112 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2-995].

important to note that the ALRC's recommended approach in respect of existing customers includes the ability to opt out at any time, discussed below.

26.84 The concept of an existing customer should require some kind of ongoing commercial, contractual or business relationship. The question of whether someone is an existing customer should be determined by reference to the particular factual circumstances. Generally, however, a one-off purchase would not be sufficient to make an individual an existing customer—such a conceptualisation of an existing customer would be too loose. This is consistent with the approach taken under both the *Spam Act* and the *Do Not Call Register Act.* In the ALRC's view, however, the concept of existing customer would generally allow for the direct marketing of products and services other than those previously provided to the existing customer.

26.85 The question of whether someone is an existing customer also needs to be resolved by reference to the particular organisation in question—that is, an individual who is an existing customer of a particular organisation will probably not be an existing customer of a related body corporate of that organisation. In this regard, the ALRC adopts the reasoning of the *Do Not Call Register Act*. The effect of this is that direct marketing communications from related bodies corporate should be treated as unsolicited direct marketing communications.

26.86 The concept of 'reasonable expectation' is an appropriate way to anchor the requirements applying in the context of existing customers. The ALRC notes that the concept of reasonable expectations already exists under the *Privacy Act.* The factors relevant to determining whether a use or disclosure is within a person's reasonable expectations[113] also would be relevant to determining whether the use of personal information for the purpose of direct marketing is within the reasonable expectations of an existing customer.

26.87 In relation to individuals who are not existing customers, an organisation should use or disclose personal information about them for the purpose of direct marketing only where: the individual has consented; or the information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure. The ALRC has modelled this aspect of the principle on the existing requirements attaching to secondary purpose direct marketing under NPP 2.1(c). Further protections are warranted in relation to the use or disclosure of sensitive information for the purpose of unsolicited direct marketing and direct marketing to persons under 15 years.[114]

26.88 The concept of 'impracticability' in respect of unsolicited direct marketing under the 'Direct Marketing' principle would need to be broader than that which exists

---

113 'Reasonable expectations' in the context of use and disclosure of personal information are discussed in Ch 25.

114 This is discussed in detail below.

currently in relation to secondary purpose direct marketing. The question of whether it is possible logistically to contact the relevant individuals is not a complete answer to the question of whether it is impracticable to obtain consent. The concept of 'impracticability' is broader, and flexible enough to take into account considerations relevant to the particular circumstances. Such factors may include the number of individuals on a direct marketing list, the cost of obtaining consent and the time involved. An organisation, however, needs to be in a position to demonstrate factors which render the obtaining of consent impracticable in the particular circumstances.

Opt-in or opt-out requirement?

Background

26.89 The Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry) recommended that the ALRC consider the possibility of an 'opt-in' regime for direct marketing, in line with the *Spam Act*.[115] The OPC Review recommended that the Australian Government consider amending the *Privacy Act* to provide that consumers have a general right to opt out of direct marketing approaches at any time, and also to impose an obligation on organisations to comply with opt-out requests within a specified time after receipt.[116]

26.90 Some overseas privacy legislation, such as that in force in Hong Kong, provides for an 'opt-out' model.[117] A similar approach is taken in the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) (EU Directive).[118] A Working Party, set up under art 29 of the EU Directive, commented that 'where data are transferred for the purposes of direct marketing, the data subject should be able to "opt-out" from having his/her data used for such purposes at any stage'.[119]

26.91 In DP 72, the ALRC considered whether the relevant privacy principle should adopt an opt-in regime, an opt-out regime, or neither. In other words, should organisations engaged in direct marketing be required to allow individuals to opt out of receiving direct marketing communications; should organisations only be permitted to engage in direct marketing if the individual in question has explicitly opted in to receiving such communications; or should neither of these requirements apply? The ALRC proposed that the 'Direct Marketing' principle should require organisations to

---

115 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 15.

116 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 23.

117 See *Personal Data (Privacy) Ordinance* (Hong Kong) s 34.

118 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 14(b).

119 European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998, ch 1.

present individuals with a simple means to opt out of receiving direct marketing communications.[120]

Submissions and consultations

26.92 This proposal was supported by the majority of stakeholders who commented on it.[121] ANZ submitted that the current opt-out provisions were working well. ANZ noted that it communicates regularly with its customers about services and products that may be beneficial to a customer's circumstances and that ANZ customers can contact it at any time if they do not want to receive further direct marketing communications.[122] BPay submitted that no change should be made to the existing opt-out mechanism under the NPPs, which provide adequate protection of the privacy of individuals.[123]

26.93 Some stakeholders called for an opt-in model.[124] The Consumer Action Law Centre submitted that, while it believes there is a strong consumer argument for an opt-in model, 'any opt-out model of regulating direct marketing must be clear and simple to use and should ensure that consumers who do not want to be contacted by direct marketers are not contacted'.[125]

26.94 The Victorian Council for Civil Liberties submitted:

> The discussion in the Review appears to start from the principle or policy position that passing on non-sensitive information for the purposes of direct marketing is permissible provided that the individual is given an opportunity to request to be taken off direct marketing lists. Liberty Victoria believes that at the very least all direct marketing should provide an opt-out mechanism.[126]

26.95 Some of the support for the ALRC's proposal was qualified. For example, the Law Council supported the concept of an opt-out model in principle, but argued that the concept of a simple means to opt out needed to be amplified.[127] The Australian Privacy Foundation and the Cyberspace Law and Policy Centre supported the opt-out

---

120 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 23–3, 23–4.

121 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Pureprofile, *Submission PR 526*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Information Industry Association, *Submission PR 410*, 7 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; B Laing, *Submission PR 339*, 12 November 2007.

122 ANZ, *Submission PR 467*, 13 December 2007.

123 BPay, *Submission PR 566*, 31 January 2008.

124 Confidential, *Submission PR 535*, 21 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

126 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.

127 Law Council of Australia, *Submission PR 527*, 21 December 2007.

model, but suggested that it be strengthened in particular ways.[128] They argued that there should be a specific requirement that the provided means to opt out be 'functional'—that is, able to achieve the intended effect. This would be similar to the 'functional unsubscribe facility' requirement in the *Spam Act*. They also argued that there should be a specific reference to an individual's ability to opt out indirectly.[129] The Cyberspace Law and Policy Centre submitted that this should occur through 'any general preference scheme to which the organisation or agency is subject' and it should ensure that organisations and agencies respect individual's preferences registered with such schemes as the Do Not Call Register or the voluntary ADMA Do Not Mail Service.[130] The Cyberspace Law and Policy Centre also argued that the principle should not use technology or media-specific language.[131]

26.96 Optus also expressed qualified support. It agreed that individuals should have a general right to opt out, but argued:

> The 'Direct Marketing' principle should not require organisations to draw attention to the ability to opt-out in each direct marketing communication with the individual. This may have been appropriate at the introduction of the private sector provisions of the *Privacy Act* however many individuals are now aware of their rights with respect to the use and disclosure of their information and this is no longer necessary.
>
> Australian individuals are able to and frequently do articulate that they do not want to be contacted by an organisation for direct marketing purposes. This occurs regardless of whether they are aware of their rights under the *Privacy Act* or not and regardless of whether they are a potential customer or an existing customer.[132]

26.97 Similarly, ADMA did not support the proposal that organisations be required to present individuals with the opportunity to opt out with each marketing approach, as this ignored the need for organisations to communicate with their existing customers to 'fulfil their wants and needs'. In ADMA's view, such a requirement would have an inconsistent impact on marketing channels—for example, it would unfairly impact on organisations that rely on telephone marketing by effectively introducing an opt-in approach for telemarketing calls. ADMA argued that this would place Australian businesses at a 'distinct commercial disadvantage' globally. ADMA's view was that the introduction of 'different provisions for current or prospective customers, and prescriptive definitions of the circumstances where an opt-out opportunity must be provided for each would be onerous'. Instead, it submitted that 'individuals should

---

128 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

129 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

131 Ibid.

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

have the right to opt-out *on request* and the organisation in question should comply with that request within a reasonable period of time'.[133]

ALRC's view

26.98 The majority of stakeholders expressed support for an opt-out model to regulate direct marketing under the *Privacy Act*. This support was expressed by a broad range of stakeholders, including individuals, some entities directly or indirectly involved in direct marketing, the OPC and privacy advocates. Nevertheless, some concern was expressed that an opt-out model which required an organisation to provide an individual with an opportunity to opt out with each direct marketing communication would be too restrictive on businesses that use direct marketing, particularly with respect to communications with existing customers.

26.99 Organisations should be required to provide a simple and functional means by which an individual (whether or not an existing customer) may advise the organisation that he or she does not wish to receive any further direct marketing communications. An individual should be able to make use of such means to opt out of further direct marketing communications at any time. The ALRC's recommended 'Direct Marketing' principle addresses the concerns raised by stakeholders by requiring organisations to provide a simple and functional means to opt out and by adopting media neutrality.[134]

26.100 There is a legitimate basis for drawing a distinction between unsolicited direct marketing and direct marketing to existing customers, in terms of the frequency with which express opportunities to opt out must be provided by organisations. An organisation should be required to provide an individual with an opportunity to opt out of receiving further direct marketing communications in every direct marketing communication which is unsolicited or directed to an individual under 15 years. This requirement is modelled on the existing requirement under NPP 2.1(c)(iv). An organisation should be required to draw to the individual's attention, or prominently display a notice, advising the individual that he or she may express a wish not to receive any further direct marketing communications. This requirement is warranted by the high level of community concern about unsolicited direct marketing. This requirement, however, is not necessary for existing customers. It should be sufficient for existing customers to be made aware, through an organisation's Privacy Policy, that they have the ability to opt out of direct marketing communications at any time.

Application of the principle to individuals under 15 years of age

26.101 In DP 72, the ALRC considered whether direct marketing may pose a particular risk to children and young people. It noted the submission of the Obesity Prevention Policy Coalition and Young Media Australia, that 'children are more susceptible to commercial manipulation than adults'. These problems are exacerbated

---

133 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007. See also Acxiom Australia, *Submission PR 551*, 1 January 2008.

134 Media neutrality means that the principle does not use technology or media-specific language.

by a number of factors, including that children and young people often 'lack the cognitive capacity and maturity' to give informed consent, and also that new technologies (such as the internet, email and SMS) are increasingly being used in direct marketing to children. For this reason, the Obesity Prevention Policy Coalition and Young Media Australia submitted that organisations should be prohibited from engaging in direct marketing with a child under 14 years, unless a parent has provided 'express and verifiable consent'.[135]

26.102 In DP 72, the ALRC stated that the proposed 'Direct Marketing' principle would provide sufficient protection by building in a consent mechanism, combined with the proposals regarding decision making on behalf of individuals under the age of 15. The ALRC proposed that OPC guidance should address direct marketing in respect of particularly vulnerable individuals.[136]

Submissions and consultations

26.103 A number of submissions addressed the application of the 'Direct Marketing' principle to children. These submissions are considered in detail in the general discussion of privacy issues impacting on children and young people in Chapter 69.

26.104 For example, the Obesity Policy Coalition continued to express concern about direct marketing to children and the way in which it should be regulated by the *Privacy Act*. It submitted that the proposed 'Direct Marketing' principle, and OPC guidance, would impose insufficient obligations on organisations; and too easily allow organisations to avoid the consent requirement where 'it is difficult to identify, locate or communicate' with the person with parental responsibility.[137]

26.105 The Obesity Policy Coalition also was concerned about the effective operation of the opt-out provisions of the proposed 'Direct Marketing' principle. While indicating 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 a child or young person, the Coalition expressed concern that ongoing communication directly between the organisation and the child or young person may impede 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 receive the opt-out information directly each time information is communicated to that child or young person.[138]

---

135 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144*, 25 January 2007.
136 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 23–6.
137 Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.
138 Ibid.

ALRC's view

26.106 The ALRC recognises that children and young people particularly can be at risk from direct marketing. In reformulating the 'Direct Marketing' principle, the ALRC has considered the level of protection that exists for children and young people. Part of the ALRC's reasoning in DP 72 for not imposing additional protections for children and young people in relation to direct marketing was that the proposed principle operated so as to, in effect, require parental consent before using personal information about a child or young person for the purposes of direct marketing. The ALRC acknowledged that the proposed exception to consent—that is, where it is non-sensitive information and it is impracticable to obtain consent—would apply, but proposed guidance to indicate how the exception would operate so as to limit organisations claiming in inappropriate circumstances that it is impracticable to obtain parental consent.[139]

26.107 It is appropriate that, as a general approach, parental consent should be a prerequisite to using the personal information of a child or young person under the age of 15 for direct marketing purposes.[140] While, overall, the ALRC considers that the obligations in relation to direct marketing to existing customers can be reduced due to the ongoing relationship between the organisation and customer, this policy is not appropriate when dealing with children and young people under the age of 15. It is very likely that these customers do not have the ability to comprehend the nature of an ongoing relationship or have sufficient understanding to meet the criterion of a 'reasonable expectation' of receiving direct marketing as a result of that continuing relationship.

26.108 To address these concerns, the ALRC's recommended 'Direct Marketing' principle provides further protection for individuals under the age of 15 years. The principle will require that direct marketing to individuals under the age of 15 years can only occur where either: the individual has consented; or the information is not sensitive information, and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure. An individual under the age of 15 should always be treated as an individual who is not an existing customer. 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. For example, an opportunity to opt out of receiving further direct marketing communications must be provided each time information is communicated to that child or young person. Further, combined with the ALRC's recommendations relating to decision making for children and young people under the age of 15, it will require that a person with parental responsibility provide the consent

139 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [60.136].
140 See Ch 69.

on behalf of the child or young person.[141] Particular privacy issues affecting children and young people, including direct marketing, are discussed in Chapter 69.

26.109 Some stakeholders had concerns about the operation of the 'not practicable' exception to obtaining consent in the 'Direct Marketing' principle, and the likely detrimental effect this would have on organisations implementing appropriate age verification and parental consent mechanisms. The ALRC notes these concerns and considers it will be necessary to ensure that guidance in relation to the 'Direct Marketing' principle addresses such concerns to ensure that the principle and provisions are implemented appropriately.[142] This is discussed below.

Recommendation 26–3 The 'Direct Marketing' principle should provide 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 only where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and

(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 direct marketing communications.

Recommendation 26–4 The 'Direct Marketing' principle should provide that 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 only in the following circumstances:

(a) either:

  (i) the individual has consented; or

  (ii) the information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;

(b) 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 direct marketing communications; and

141 Rec 68–1. See also Recs 68–2, 68–3, 68–4.

142 See recommendations in relation to guidance in these areas: Recs 26–7, 68–4.

(c) 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 direct marketing communications.

Timeframes for compliance with opt-out requests

26.110 In DP 72, the ALRC considered whether direct marketers should be required to comply with an opt-out request within a set timeframe. That is, when a person expresses their intention to opt out of receiving direct marketing communications, should the organisation be required to comply with this request within a period specified in the 'Direct Marketing' principle? There was no consensus among those who favoured a specified timeframe. One view was that any such timeframe should be consistent with the *Spam Act*, which provides for five business days within which to act upon the request.[143] On the other hand, in the OPC Review, the OPC approved of ADMA's view that the period should be 45 days.[144]

26.111 The ALRC proposed, in DP 72, that an organisation should be required to comply within a 'reasonable time' with an individual's request not to receive direct marketing communications.[145]

Submissions and consultations

26.112 The ALRC's proposal was supported by the majority of stakeholders.[146] ADMA commented that:

> It is current industry best practice that in all instances, including where an ongoing business relationship exists between the organisation and the individual, that an organisation respects and actions an individual's request to opt-out of future direct marketing approaches.[147]

26.113 The Law Council submitted that the concept of a 'reasonable time' was a 'sensible approach', since different direct marketing channels (for example, email as opposed to post) have different timeframes.[148] Optus submitted that five days for implementation of an 'opt-out' request was too short.[149]

---

143 See *Spam Act 2003* (Cth) sch 2, cl 6(1).

144 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 100.

145 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 23–3, 23–4.

146 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Obesity Policy Coalition, *Submission PR 506*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

147 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

148 Law Council of Australia, *Submission PR 527*, 21 December 2007.

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

26.114 The DBCDE noted that the five day time limit in the *Spam Act* applies differently depending on the communication medium used. If a withdrawal of consent is sent electronically, the five day time limit starts on the day on which the message was sent, but if a request is sent by post, the time limit does not commence until service of the message is effected. In any other case, the time limit does not commence until the day on which the message is delivered. On this basis, it submitted that the *Spam Act* provided for a flexible response.[150]

26.115 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre supported the proposal, but urged that it be 'strengthened by prescription, in Regulations or a binding Code, of specific target response times for different media of communication'.[151]

26.116 While the OPC expressed general support, its view was that an organisation involved in direct marketing should comply with an individual's request not to receive direct marketing communications within 'a specific period of time'. It suggested that other sectoral legislation could provide guidance as to the time period.[152] PIAC shared this view, submitting that a 'reasonable time' requirement is 'too vague and open to self-serving interpretations by direct marketing organisations'.[153]

ALRC's view

26.117 In order to make the opt-out model effective, the 'Direct Marketing' principle should provide that organisations must act on a request by an individual not to receive any further direct marketing communications within a reasonable period of time. The term 'reasonable' should be interpreted with reference to all relevant factors, including how the direct marketing communications are transmitted and the length of time it takes to amend an organisation's database. It is too difficult to specify a time period that addresses all of the ways in which direct marketing communications can occur. The wide variation in the timeframes suggested by stakeholders illustrates this point. The 'Direct Marketing' principle should not specify the number of days within which to act on any request not to receive direct marketing communications. Rather, the organisation should comply within a reasonable time.

26.118 The 'Direct Marketing' principle should clarify that an organisation must not charge an individual for giving effect to a request from the individual not to receive further direct marketing communications. This currently forms part of NPP 2.1(c)(ii) and it is important that this requirement be retained.

---

150 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007. DBCDE noted that the Department's recent review of the *Spam Act* concluded that the arrangements were appropriate.

151 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

153 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

Recommendation 26–5 The 'Direct Marketing' principle should provide that an organisation involved in direct marketing must comply, within a reasonable period of time, with an individual's request not to receive further direct marketing communications and must not charge the individual for giving effect to such a request.

Original source of personal information

26.119 The OPC Review recommended that the Australian Government consider amending the *Privacy Act* to require organisations engaged in direct marketing to take reasonable steps, on request, to advise an individual from where it acquired the individual's personal information.[154] In its submission to the OPC Review, ADMA stated that the rationale behind such a provision is that 'informing individuals of the source of the data being used gives them more control over their personal information and reduces the number of repeat complaints about unsolicited marketing'.[155] A recent survey commissioned by the OPC indicated that 53% of people who had received unsolicited direct marketing communications were concerned about how the organisations in question obtained their details.[156]

26.120 One individual who contacted the ALRC noted:

> Some marketing organisation has gotten my details for on-selling, but I can't get at the 'source'. I can only tell marketers who contact me directly to remove my name from their individual lists. I want for the 'source' to be obliged to tell me on a regular basis … what details they have on me, and give me the chance to have my details removed from their master list.[157]

26.121 In DP 72, the ALRC proposed that the 'Direct Marketing' principle should provide that an organisation involved in direct marketing, when requested by an individual to whom it has sent direct marketing communications, must take reasonable steps to advise the individual from where it acquired the individual's personal information.[158]

---

154 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 24.

155 Ibid, 101–102.

156 Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), 29.

157 Anonymous, *Submission PR 189*, 10 February 2007. See also E Cousins, *Submission PR 585*, 11 April 2008.

158 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 23–5.

Submissions and consultations

26.122 A range of views were received on the ALRC's proposal. A large number of stakeholders expressed support for the proposal,[159] including the OPC which stated:

> This proposal would enhance transparency in how individuals' personal information is handled and promote handling that accords with individuals' reasonable expectations … Knowing the source of the information may also permit the individual to pursue other options with that entity, such as to complain to it or, if the entity is an agency or organisation, make a complaint about the disclosure to the Privacy Commissioner.[160]

26.123 PIAC also expressed strong support, arguing that it would 'empower individuals to take back control' of the use of their personal information. PIAC noted that it also may encourage organisations to 'carefully consider whether they have a legitimate basis for collecting the personal information in the first place'.[161]

26.124 The Victorian Council for Civil Liberties identified as a central issue

> where the 'master source' of the information discloses it to a number of direct marketing bodies resulting in an individual being inundated with information they neither sought nor are interested in. In such cases the individual needs to identify the source in order to be removed from the Master list.[162]

26.125 The Consumer Action Law Centre submitted that:

> marketers should be obliged to inform individuals, on request, of the source of the individual's personal information … Consumers are often frustrated by companies failing to tell them where they obtained their personal information.[163]

26.126 While the Cyberspace Law and Policy Centre and the Australian Privacy Foundation supported the proposal, they called for more specificity 'by requiring information on the identity of the source', arguing that, in its absence, 'the principle could be satisfied by a broad generic description—for example, a of list brokers'. This would be of limited value to an individual seeking to 'follow the chain' of information.[164]

---

159 GE Money Australia, *Submission PR 537*, 21 December 2007; Pureprofile, *Submission PR 526*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Obesity Policy Coalition, *Submission PR 506*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

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

161 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

162 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007. Also, one individual raised concerns about their personal information being sold to 'name brokers' without permission: E Cousins, *Submission PR 585*, 11 April 2008.

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

164 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

26.127 AMCA submitted that the proposal was generally consistent with the requirements placed on persons making telemarketing and research calls under the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007* (Cth) (the Industry Standard).[165] ACMA noted that the Industry Standard requires telemarketers and researchers (the callers), if requested by the call recipient, to indicate where they obtained the telephone number and the name and contact details of any organisation that provided them with the information (where applicable). ACMA also noted that the requirements only apply to data disclosed to a caller after 1 July 2007.[166]

26.128 Optus expressed support for the proposal. It submitted, however, that the requirement should be limited to requiring an organisation to provide an individual with the contact details of the company from which the organisation sourced the data.

> Should an individual want to trace the source of their data the responsibility to conduct this activity should fall to the individual and individuals should be given sufficient information to conduct this activity. A requirement for organisations to obtain and hold the primary source of data would be extremely expensive and cause a significant increase in the compliance costs of the *Privacy Act*.[167]

26.129 ADMA's support for the proposal was qualified. It agreed that 'retaining records regarding the source of contact details and disclosing the source to the consumer on request is best practice and should be encouraged' but called for a 'balanced and logical approach'. It submitted that many organisations currently lack the capacity to store information about the source of contact details. ADMA sought two modifications to the ALRC's proposal: the requirement should apply to contact details only, rather than all personal information held by an organisation; and the obligation must not apply retrospectively, because most organisations do not currently hold these records and it would not be possible for them to comply.[168]

26.130 There also were a number of stakeholders that objected to the proposal.[169] The ABA raised a number of issues. First, it asked whether it would be necessary to name a 'precise source' or whether it was intended that reference to a 'generic source' would be sufficient, such as 'from a credit bureau'. Secondly, it noted that there may be

---

165 *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007* (Cth) as amended by the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard Variation 2007 (No 1)* (Cth).

166 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

167 Optus, *Submission PR 532*, 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; BPay, *Submission PR 566*, 31 January 2008; Confidential, *Submission PR 536*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007.

problems where information is collected from multiple sources, including unsolicited sources.[170]

26.131 BPay strongly disagreed with the proposal, on the basis that 'many organisations would have great difficulty in complying' and because of the 'large expense associated with developing systems to comply with this proposal'.[171] The Law Council of Australia submitted that the proposal was 'impracticable' and 'burdensome' on organisations. Further, it submitted:

> If such a requirement is introduced, it should only oblige an organisation to advise the individual of the direct source from which the organisation acquired the data (and not the original source of the data), and should not require the organisation to make any further enquiries beyond this source.
>
> The requirement should not apply retrospectively; particularly given the source information may not have been recorded and therefore may not be ascertainable by some organisations.[172]

26.132 Microsoft Asia Pacific also argued that the implementation of the proposal has the potential to result in substantial costs. Such costs are likely to arise from: a change to 'business practices and systems to ensure that source data is collected'; and the fact that businesses will be required to 'record and maintain data about all of the multiple sources from which they collect personal information'. Microsoft indicated that, in its experience, personal information is collected and updated from numerous sources. For this reason, substantial resources would be required to 'record source data on each occasion that personal information is collected or updated'. It called on the ALRC to weigh the costs associated with the proposal against the privacy benefits it was likely to generate, arguing that the proposal was an 'unduly onerous step' when the likely costs were taken into account.[173]

26.133 Telstra objected to the proposal on the basis that 'it creates significant obligations on organisations but gives no significant benefit to individuals' privacy'. In Telstra's view, having to track information from the 'point of entry into the organisation' until it was used for direct marketing purposes would involve a significant compliance burden.

> The complexity of undertaking this task increases further if the information is obtained through other organisations which themselves have collected information through various sources. It is very different to a simple scenario in which an organisation buys a customer list and uses the personal information acquired from that list for marketing purposes. This scenario is, we believe, relatively unusual.[174]

---

170 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Law Council of Australia, *Submission PR 527*, 21 December 2007.

171 BPay, *Submission PR 566*, 31 January 2008.

172 Law Council of Australia, *Submission PR 527*, 21 December 2007.

173 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

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

26.134 One stakeholder in the airline industry highlighted the practical constraints for organisations in complying with the ALRC's proposal. It noted that often organisations collect many separate pieces of information about their customers and that compliance would be expensive, for example, as a result of the costs associated with the storage of information. The stakeholder also noted that sometimes compliance would be impossible. An example noted was Global Distribution Systems.[175] Global Distribution Systems are 'international computer reservations systems that book and sell tickets for most airlines'—there are four major suppliers of such systems internationally. No travel business has control over the information that such a system records, except to the extent that they themselves enter it. It would be unlikely that any major Global Distribution System would be prepared to take on the 'major development costs (both in terms of modification of software and data storage)' in order to comply with such a requirement.[176]

ALRC's view

26.135 Many stakeholders were in favour of requiring organisations involved in direct marketing to take reasonable steps, on request, to advise an individual from where they acquired the individual's personal information.

26.136 Such a requirement would be useful particularly where an individual's personal information has been disclosed by an organisation to another organisation and it has then been used to carry out unsolicited direct marketing. In such a situation, the individual could follow a 'chain' of disclosure to the source and, if he or she wished, could then take action to have his or her name removed from the list. This would facilitate individuals being able to assert substantive, as distinct from merely formal, privacy rights with respect to direct marketing.

26.137 Part of the Terms of Reference for this Inquiry called for the ALRC to consider the 'desirability of minimising the regulatory burden on business in the privacy area'.[177] The ALRC does not want to add unnecessarily to the compliance burdens faced by organisations.

26.138 The recommended 'Direct Marketing' principle provides, therefore, that this requirement will only apply where the direct marketing communications are made to individuals who are not existing customers. In the ALRC's view, concern about source will be most relevant where there is no existing business relationship between an organisation and an individual.

26.139 Further, the recommended 'Direct Marketing' principle introduces a 'reasonable and practicable' threshold. The ALRC acknowledges that there may be constraints on an organisation's ability to provide source information and, in some

175 Confidential, *Submission PR 536*, 21 December 2007.
176 Ibid.
177 The Terms of Reference are reproduced at the beginning of this Report.

cases, it may not be practicable to provide such information. In other circumstances, to provide source information may not be reasonable. In deciding whether it is reasonable to provide source information, relevant factors may include the potential consequences to the individual if the information is not provided—for example, that the individual may continue to receive unsolicited direct marketing communications—and the cost to the organisation of providing this information.

26.140 For these reasons, the ALRC recommends that an organisation who has made direct marketing communications to an individual who is not an existing customer must, where reasonable and practicable and where requested to do so by the individual, advise the individual of the source from which it acquired the individual's personal information.

26.141 'Source' in this context should mean the direct source from which the organisation acquired the information. For example, if organisation C obtains personal information from organisation B, who in turn obtained the personal information from organisation A, organisation C, in responding to a request for source information, will only need to disclose the details of organisation B. It would be unduly onerous to require organisations to track personal information back to the original source. In some cases, organisation C may not be aware that organisation B obtained the personal information from some other source.

Recommendation 26–6 The 'Direct Marketing' principle should provide that an organisation that has made direct marketing communications to an individual who is not an existing customer or is under 15 years of age must, where reasonable and practicable and where requested to do so by the individual, advise the individual of the source from which it acquired the individual's personal information.

Direct marketing to vulnerable individuals

26.142 Concerns have been raised about the practice of sending direct marketing communications to vulnerable people in the community. For example, direct marketing may pose a particular risk to children, young people and adults with a decision-making disability because their cognitive faculties may be less developed than those of other people, making it more likely that they will be manipulated. Changes to the 'Direct Marketing' principle to make further provision in respect of direct marketing to children and young people are discussed above.

26.143 Direct marketing can be insensitive where an error in a personal information database causes direct marketing communications to be sent, for instance, to a grieving friend or relative of a deceased individual. One individual stated that it can be traumatic to receive direct marketing communications addressed to her late husband, and this should be rectified by requiring organisations involved in direct marketing to

update their databases regularly.[178] The ALRC Phone-In also received a number of calls stating that direct marketing can be frightening for older people.

26.144 The question arises whether reform is desirable to address these issues. In DP 72, the ALRC proposed that the most appropriate mechanism to alleviate this problem would be guidance issued by the OPC about direct marketing to particularly vulnerable individuals.[179] The ALRC also proposed that the OPC should issue guidance to organisations engaged in direct marketing to highlight their obligations in relation to data quality, and assist them with information on how best to fulfil those obligations.

Submissions and consultations

26.145 The provision of guidance in respect of particularly vulnerable individuals was supported by the majority of stakeholders who commented on the issue.[180] Some stakeholders called for a stronger response in respect of direct marketing to children and young people.[181]

26.146 Some concern was expressed by stakeholders about the proposal for OPC guidance in respect of data quality obligations in the context of direct marketing. For example, Acxiom submitted that, while it would be beneficial for the OPC to develop guidance relating to an organisation's responsibility to maintain the quality of any database containing personal information, 'this guidance should apply to all organisations that are subject to the UPPs, not solely to organisations that use personal information for direct marketing'.[182] GE Money submitted that it was not clear why the proposed 'Data Quality' principle would not be a sufficient general standard and why organisations involved in direct marketing require specific guidance on issues relating to data quality.[183]

ALRC's view

26.147 The OPC should issue guidance to help organisations understand better how to direct market appropriately to vulnerable individuals. In particular, this guidance should help to clarify the obligations of an organisation when dealing with vulnerable

---

178 A Baxter, *Submission PR 74*, 5 January 2007.

179 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 23–6.

180 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Optus, *Submission PR 532*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 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; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

181 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Obesity Policy Coalition, *Submission PR 506*, 20 December 2007.

182 Acxiom Australia, *Submission PR 551*, 1 January 2008.

183 GE Money Australia, *Submission PR 537*, 21 December 2007.

people, such as the elderly, individuals with a decision-making disability and individuals under the age of 15.[184]

26.148 The focus of guidance in the context of direct marketing to children and young people should be on consent and, specifically, when it will be impracticable to seek consent. The interpretation of these concepts is critical to ensuring that privacy protection in the context of direct marketing to children and young people is preserved.

26.149 Where communication by direct marketing can itself be traumatic—for example, where communications are addressed to a deceased individual and received by that individual's grieving friend or relative—the issue relates most directly to the 'Data Quality' principle. As discussed in Chapter 27, the 'Data Quality' principle requires that all personal information that is collected, used or disclosed by an agency or organisation be 'accurate, complete, up-to-date and relevant'. It is not necessary, therefore, for the OPC to provide guidance with respect to data quality obligations as they relate to direct marketing.

Other OPC guidance

26.150 The ALRC's recommended 'Direct Marketing' principle introduces a new framework for the regulation of direct marketing. In particular, the principle turns on the concept of an 'existing customer' and introduces a new requirement relating to the source of personal information used for the purpose of direct marketing.

26.151 In the ALRC's view, OPC guidance is required in a number of areas. This guidance should address what constitutes an 'existing customer'. It is important that the parameters of what constitutes an existing customer are delineated clearly, so as to ensure the effective operation of the 'Direct Marketing' principle. This guidance also should address the types of direct marketing communications which are likely to be within the reasonable expectations of existing customers and the extent to which the use and disclosure of sensitive information for the purposes of direct marketing will be within an existing customer's reasonable expectations. The OPC also should provide guidance about the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing.

26.152 It is important that OPC guidance also address the factors for an organisation to consider in determining whether it will be reasonable and practicable to advise an individual of the source from which it acquired the individual's personal information. Such factors may include the privacy consequences to the individual if the information is not provided and the cost to the organisation of providing this information.

184 This will need to be consistent with other guidance for children and young people: see Chs 68, 69.

Recommendation 26–7 The Office of the Privacy Commissioner should develop and publish guidance to assist organisations in complying with the 'Direct Marketing' principle, including:

(a) what constitutes an 'existing customer';

(b) the types of direct marketing communications which are likely to be within the reasonable expectations of existing customers;

(c) the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing to an individual who is not an existing customer or is under the age of 15 years;

(d) the factors for an organisation to consider in determining whether it is reasonable and practicable to advise an individual of the source from which it acquired the individual's personal information; and

(e) the obligations of organisations involved in direct marketing under the *Privacy Act* in dealing with vulnerable people.

Summary of 'Direct Marketing' principle

26.153 The Direct Marketing principle in the model UPPs should be called 'Direct Marketing'. It may be summarised as follows.

UPP 6. Direct Marketing (only applicable to organisations):

6.1 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 only where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and

(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.

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 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;

(b) 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;

(c) 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

(d) 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.

6.3 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.

27. Data Quality

Contents

Introduction

27.1 In this chapter, the ALRC recommends that a ‘Data Quality’ principle, applicable to agencies and organisations, should be included in the model Unified Privacy Principles (UPPs). The ALRC considers a number of changes from the present data quality obligations set out in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs). In particular, it recommends that agencies and organisations should take steps to ensure that the personal information they collect, use and disclose is ‘relevant’. The ALRC also considers the interaction between the ‘Data Quality’ principle and other obligations set out in the model UPPs.

Background

27.2 The *Privacy Act 1988* (Cth) contains provisions that are designed to ensure that, where an agency or organisation handles personal information, it takes reasonable steps to make certain that the information is of a sufficiently high quality—that is, that the information is accurate, complete, up-to-date and (for agencies) relevant. These are commonly known as ‘data quality’ requirements. Ensuring the quality of personal

information that is collected, used and disclosed, is recognised as a fundamental obligation of agencies and organisations under the *Privacy Act*.[1]

27.3 NPP 3 provides that:

> An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.[2]

27.4 The IPPs do not contain a 'stand-alone' data quality principle that applies to agencies. Aspects of the data quality principle, however, are included in IPPs 3 and 8. IPP 3 provides that, where an agency collects personal information, it must

> take such steps (if any) as are in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected … the information collected is relevant to that purpose and is up-to-date and complete.[3]

27.5 IPP 8 provides that an agency

> who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up-to-date and complete.[4]

27.6 The IPPs do not impose data quality requirements at the time of disclosure. This differs from some overseas privacy legislation. For example, US privacy legislation requires agencies to ensure that, before disclosing a record about an individual to any person other than an agency, they make reasonable efforts to ensure that such records are 'accurate, complete, timely and relevant for agency purposes'.[5]

Application of the 'Data Quality' principle to agencies

27.7 As is noted above, agencies presently are not subject to a discrete 'Data Quality' principle. In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that a single 'Data Quality' principle should apply to both agencies and organisations.[6]

---

1 See, eg, Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General), 2117; Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 141.

2 *Privacy Act 1988* (Cth) sch 3, NPP 3.

3 Ibid s 14, IPP 3. This requirement only applies to 'solicited' personal information.

4 Ibid s 14, IPP 8.

5 *Privacy Act 1974* 5 USC § 552a (US). See also G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 5 May 2008, Principle 10.

6 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 25–1.

27.8 The proposal was supported almost unanimously by stakeholders.[7] The Public Interest Advocacy Centre (PIAC), for example, submitted that

> the uneven treatment of agencies and organisations in relation to data quality requirements has been a source of confusion in the *Privacy Act*. A single principle dealing with data quality for both agencies and organisations would lead to greater consistency and increased public confidence in agency handling of personal information.[8]

27.9 Privacy NSW supported the proposal, but suggested that the 'Data Quality' principle and the 'Data Security' principle could be combined, so that agencies and organisations would only need to have reference to one principle dealing with the quality and security of record keeping.[9]

ALRC's view

27.10 The model UPPs should include a 'Data Quality' principle that applies to agencies and organisations. Placing comprehensive data quality obligations will lead to greater consistency of, and increased public confidence in, the handling of personal information. A single 'Data Quality' principle also is consistent with the ALRC's recommendation that, unless there is a sound policy reason to the contrary, the privacy principles should equally to agencies and organisations.[10]

Scope of the 'Data Quality' principle

Background

27.11 The scope of the data quality requirements set out in the IPPs and the NPPs varies in a number of respects. First, the application of the IPPs and the NPPs to information outside the possession or control of an agency or organisation differs. Pursuant to NPP 3, organisations must take steps to ensure the quality of personal information that they 'collect, use or disclose'. In comparison, the data quality obligations under IPP 8 apply to documents in an agency's 'possession or control'.

---

7 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 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; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007. In addition, the Australian Direct Marketing Association submitted that it did not disagree with this proposal. Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

8 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

9 Privacy NSW, *Submission PR 468*, 14 December 2007.

10 Rec 18–2.

Unlike NPP 3, this imposes data quality requirements on an agency that has outsourced the handling of personal information to another agency or organisation, as well as on an agency that merely holds personal information on behalf of someone else.

27.12 Secondly, the criteria in the IPPs and the NPP to ensure the quality of personal information differ. NPP 3 requires organisations to keep personal information 'accurate, complete and up-to-date'. It does not include a requirement for the information to be 'relevant'. In contrast, the IPPs contain an express provision stating that, at the time of collection, personal information must be relevant to the purpose of collection.[11] There also is a stand-alone IPP requiring that personal information only be used for relevant purposes.[12]

27.13 Finally, IPP 3 provides that the quality of personal information that agencies collect should be interpreted with regard to 'the purpose for which the information is collected'. Similarly, IPP 8 sets out that the requirements of the principle should be interpreted 'having regard to the purpose for which the information is proposed to be used'. NPP 3 does not include an equivalent framework for interpreting how its data quality criteria are to be applied.

27.14 These differences need to be addressed when considering the appropriate scope of the 'Data Quality' principle in the model UPPs.

Submissions and consultations

27.15 In DP 72, the ALRC proposed that the 'Data Quality' principle

> should require an agency or organisation to take reasonable steps to make sure that personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the proposed UPPs, accurate, complete, up-to-date and relevant.[13]

27.16 Many stakeholders supported the proposed 'Data Quality' principle.[14] The Australian Government Department of Disability Housing and Community Services and the National Health and Medical Research Council strongly supported the

---

11 *Privacy Act 1988* (Cth) s 14, IPP 3(c).

12 Ibid s 14, IPP 9. A criterion of 'relevance' also is included in the data quality requirements in a number of international instruments. See, for example: Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 6. See also: *Personal Information Protection Act 2004* (Tas) sch1, PIPP 3.

13 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 24–2.

14 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Anglicare Tasmania, *Submission PR 514*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007.

proposal.[15] The Australian Government Department of Agriculture, Fisheries and Forestry noted that its position would depend on the interpretation of 'reasonable steps'. For example, it questioned, whether the 'Data Quality' principle would require an agency to engage an independent third party proactively to assess all personal information.[16]

27.17 Some stakeholders supported expressly the additional criterion that information should be 'relevant' to the purpose for which it was collected, or a permitted secondary purpose.[17] The OPC noted that, although a relevance requirement may be implicit in other privacy principles, including it expressly in the 'Data Quality' principle would provide greater clarity and promote consistency between the principles.[18] The additional criterion of 'relevance' also was supported by all of the stakeholders who commented on this issue in submissions on Issues Paper, *Review of Privacy* (IP 31).[19]

27.18 Other stakeholders, however, raised concerns about the proposed criterion of 'relevance'. The Australasian Retail Credit Association was concerned that the application of the 'relevance' criterion in the 'Data Quality' principle could be inconsistent with the requirement under the 'Collection' principle that an agency or organisation only must collect personal information that is 'necessary for one or more of its functions or activities'.[20] The Investment and Financial Services Association (IFSA) submitted that the operation of the 'Collection' principle meant that the 'relevance' requirement was superfluous. IFSA suggested that the 'relevance' requirement was regulated already by the market, as collecting irrelevant information 'wastes space and raises the ire of the consumer to the detriment of the insurer and its business'.[21] Several stakeholders submitted that agencies and organisations may need to collect personal information where the relevance of the information only becomes

---

15 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

16 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

17 Public Interest Advocacy Centre, *Submission PR 548*, 26 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.

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

19 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; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

20 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

21 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

clear sometime after collection.[22] This could arise particularly in the context of law enforcement[23] and consular activities.[24]

27.19 Medicare Australia and Privacy NSW specifically supported including a reference to a 'purpose of collection permitted by the proposed UPPs' in the 'Data Quality' principle.[25] The Cyberspace Law and Policy Centre submitted, however, that the proposed wording of this provision should be changed. It noted that, if personal information is being used for a secondary purpose, then the agency or organisation should be required to ensure that it is of appropriate quality for that use or disclosure. This may be quite different from the 'relevance' that would be required for the primary purpose of collection.[26]

27.20 PIAC and the Office of the Victorian Privacy Commissioner (OVPC) submitted that the principle should extend to information that is in the 'possession or control' of the agency or organisation.[27]

27.21 The Cyberspace Law and Policy Centre also suggested that the 'Data Quality' principle should provide that

> an organisation or agency should take reasonable steps to avoid making a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human.[28]

ALRC's view

'Possession or control'

27.22 As noted above, the data quality obligations in NPP 3 apply only when an organisation collects, uses or discloses personal information. There was some disagreement among stakeholders about whether these requirements also should apply when an agency or organisation merely controls the information.

27.23 The 'Data Quality' principle should apply to information that an agency or organisation 'collects, uses or discloses'. Extending the application of the principle to personal information merely in the control of an agency or organisation would broaden unnecessarily the data quality requirements. For example, where an organisation maintains a database containing personal information on behalf of another organisation, it would be very onerous—and often unreasonable—to expect the second

---

22 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Victoria Police, *Submission PR 523*, 21 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

23 Victoria Police, *Submission PR 523*, 21 December 2007.

24 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.

25 Medicare Australia, *Submission PR 534*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

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

27 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

organisation to maintain the data quality of the personal information in the database. The ALRC, therefore, considers that extending the data quality principle in this way would impose an unjustified compliance burden on agencies and organisations.

'Relevance'

27.24 The 'Data Quality' principle should require that, where an agency or organisation collects, uses or discloses personal information, the information should be relevant to the purpose of that collection, use or disclosure. This complements the requirement in the 'Collection' principle that personal information collected by an organisation should be 'necessary for one or more of its functions or activities'. If the purpose of collection is not necessary for one or more of the functions or activities of an agency or organisation, the requirement in the 'Collection' principle cannot be satisfied. It is logical, therefore, to include a corresponding obligation to limit the use or disclosure of personal information to that which is relevant to the purpose of that use or disclosure.

27.25 Moreover, the fact that an agency or organisation has legitimately collected personal information for a permitted purpose should not mean that it is necessarily allowed to use or disclose *all* of that information. Rather, the agency or organisation should be allowed to use or disclose only so much of the personal information it holds as is relevant to the purpose of the particular use or disclosure.

27.26 This is illustrated by the following hypothetical example. Assume that a company, X, lawfully collected personal information about an individual, Y, including her address, job description, marital status, physical disabilities and financial position. This was necessary for the purpose of providing Y with financial advice. Some time later, X wishes to disclose Y's personal information to another company, Z, for the purpose of buying shares on Y's behalf—this being a related secondary purpose that Y would reasonably expect. X should not be permitted to disclose to Z *all* the personal information it holds on Y. Instead, X should be allowed to disclose only such personal information about X as is relevant to obtaining the shares.

27.27 The other concern raised by stakeholders about including a relevance criterion in the 'Data Quality' principle was the potential for it to prevent them from collecting personal information where the relevance of the information only can be established some time after collection. The ALRC notes, however, that IPP 3 already requires agencies only to collect 'relevant' information. Furthermore, where an agency or organisation collects personal information that is 'unnecessary for one or more of its functions or activities'—and, therefore, breaches the 'Collection' principle—it is appropriate that retention of this information should be a breach of the 'Data Quality' principle. The ALRC does not consider, therefore, that including a relevance criterion in the 'Data Quality' principle would impede the legitimate functions of agencies and organisations.

Reference to permitted purpose

27.28 In DP 72, the ALRC proposed that the 'Data Quality' principle should be interpreted having regard to 'a purpose of collection permitted by the proposed UPPs'. The ALRC accepts the Cyberspace Law and Policy Centre's argument that, if an agency or organisation uses or discloses personal information for a secondary purpose, then the appropriate question is whether the information is of a quality appropriate for that use or disclosure. This may be different from the quality that would be required for the primary purpose of collection. The 'Data Quality' principle, therefore, should include a reference to 'the purpose of that collection, use or disclosure'. This phrasing also is consistent with the data quality provisions in the IPPs and the OECD Guidelines.

Automated decision-making

27.29 In Chapter 10, the ALRC recommends that the OPC should provide guidance on when it would be appropriate for an agency or organisation to involve humans in the review of decisions made by automated mechanisms. Specific reference to automated decision making in the 'Data Quality' principle would complicate the principle unnecessarily.

Balancing data quality and other privacy interests

27.30 In its review of the private sector provisions of the *Privacy Act* (the OPC Review), the OPC noted that some organisations consider that their obligations under NPP 3 to keep personal information up-to-date and accurate are absolute, and could be used to justify intruding upon an individual's privacy.[29] In other words, compliance with the 'Data Quality' principle could result in intrusions upon an individual's privacy.

27.31 A question arises, therefore, whether the 'Data Quality' principle should be amended to make it clear that the obligation to maintain data quality is qualified. An express provision to this effect is included, for example, in the data quality principles in the OECD Guidelines[30] and in Canadian privacy legislation.[31]

27.32 In the OPC Review, the OPC stated that it is not reasonable to take steps to ensure data accuracy where this has no privacy benefit for the individual. It considered that legislative amendment of NPP 3 was unnecessary, but indicated that it would issue

---

29 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 267–268.

30 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8.

31 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada), Principle 4.6.

further guidance to organisations about their obligations under NPP 3 to ensure a proportional approach is taken to compliance.[32]

27.33 This approach was supported by a large number of stakeholders that made submissions in response to IP 31[33] and DP 72.[34] The Australian Privacy Foundation and the Cyberspace Law and Policy Centre also suggested that a statement should be included in a note to the principle or in the relevant Explanatory Memorandum that, in assessing what is 'reasonable' in the context of the 'Data Quality' principle, regard should be given to the potential for errors to result in detrimental consequences for the individual whose personal information is held.[35]

ALRC's view

27.34 Many stakeholders submitted that it was unnecessary for the 'Data Quality' principle to make it clear that there is no absolute obligation on agencies and organisations to ensure that personal information they collect, use or disclose is up-to-date and accurate.

27.35 In the ALRC's view, it is unnecessary to insert a note or include in the Explanatory Memorandum a provision that stipulates that the obligations in the 'Data Quality' principle are not absolute. Such a note or provision runs the risk of causing more confusion than it resolves. The OPC has already undertaken to provide further guidance on this issue and this guidance should adequately address the issue.

---

32 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 79.

33 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; CSIRO, *Submission PR 176*, 6 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Insolvency and Trustee Service Australia, *Submission PR 123*, 15 January 2007; AXA, *Submission PR 119*, 15 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.

34 See, for example: Optus, *Submission PR 532*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

35 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

Recommendation 27–1 The model Unified Privacy Principles should contain a principle called 'Data Quality' that requires an agency or organisation to 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.

Summary of 'Data Quality' principle

27.36 The seventh principle in the model UPPs should be called 'Data Quality'. It may be summarised as follows.

UPP 7. Data Quality

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.

28. Data Security

Contents

Introduction

28.1 In this chapter, the ALRC recommends that the model Unified Privacy Principles (UPPs) should contain a single data security principle that covers both agencies and organisations. The ALRC addresses how agencies and organisations should fulfil their data security obligations during the active life of records that contain personal information. It then examines the obligations of agencies and organisations to destroy or render non-identifiable personal information when it is no longer needed.

Background

28.2 The *Privacy Act 1988* (Cth) currently requires that agencies and organisations take reasonable steps to maintain the security of the personal information that they hold. This is commonly referred to as 'data security'. The data security requirements

for agencies and organisations are found in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) respectively.

28.3 IPP 4 provides that a record-keeper, who has possession or control of a record that contains personal information, must ensure

> (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
>
> (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of the information contained in the record.[1]

28.4 In comparison, NPP 4 provides that 'an organisation must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure'.[2] NPP 4 further requires that

> an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under [the 'Use and Disclosure' principle].[3]

28.5 Requirements to take steps to ensure the security of personal information are included in a number of international instruments relating to privacy. For example, the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* provides that

> technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.[4]

28.6 Similarly, the Security Safeguards Principle in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) provides that 'personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data'.[5] The OECD also has issued *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002), which responds to security issues raised by the interconnectivity of information systems and networks.[6]

---

1 *Privacy Act 1988* (Cth) s 14, IPP 4.
2 Ibid sch 3, NPP 4.1.
3 Ibid sch 3, NPP 4.2.
4 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 17.
5 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), art 11.
6 Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002).

Towards a single data security principle

28.7 As noted above, agencies and organisations are subject to data security requirements under the IPPs and NPPs respectively. These principles, however, differ in two main respects. First, agencies are obliged to take steps to prevent the unauthorised use or disclosure of personal information that has been disclosed to a third party in connection with the provision of a service to the agency. No equivalent obligation applies to organisations. Secondly, organisations are obliged to take steps to destroy or de-identify personal information that is no longer needed. No equivalent 'data destruction' requirement applies to agencies.

28.8 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that these differences should be reconciled in order to create a single data security principle that is applicable to agencies and organisations.[7] This proposal reflected the ALRC's broader policy of consolidating the IPPs and NPPs to create a single set of privacy principles, the UPPs, which generally would be applicable to agencies and organisations.[8]

28.9 Many stakeholders that commented on this proposal supported a single data security principle.[9] Some stakeholders suggested that the ALRC's proposed requirements for data breach notification[10] should be incorporated into the 'Data Security' principle.[11] The Australasian Compliance Institute submitted, for example, that introducing data breach notification provisions suggests that the consequences of

---

7 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 25–1.

8 Ibid, Proposal 15–2.

9 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 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; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. The Australian Direct Marketing Association did not disagree with the proposal. Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

10 See: Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 47–1.

11 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007. The ALRC's recommended data breach notification scheme is discussed in Ch 51.

non-compliance with the data security principle are not sufficient incentive to ensure compliance.[12]

ALRC's view

28.10 The model UPPs should contain a single 'Data Security' principle that applies to agencies and organisations. This will consolidate and simplify the existing provisions of the IPPs and NPPs that deal with data security. A single 'Data Security' principle also is consistent with the ALRC's recommendation that, unless there is a sound policy reason to the contrary, the privacy principles should apply equally to agencies and organisations.[13]

28.11 While the 'Data Security' principle will need to be sufficiently flexible to accommodate the differences between the operation of agencies and organisations, there is no good policy reason for maintaining two separate principles dealing with data security. The appropriateness of including, in the 'Data Security' principle, obligations that currently only apply to agencies or organisations—for example, protecting information disclosed to contractors and destroying or rendering non-identifiable information that is no longer needed—is considered below.

28.12 There is a clear connection between compliance by agencies and organisations with the 'Data Security' principle and the ALRC's recommended data breach notification provisions.[14] For example, where an agency or organisation has acted in accordance with its obligations under the 'Data Security' principle—such as taking steps to encrypt personal information—exceptions to the data breach notification provisions may apply. The deterrent effect of a data breach notification requirement also will provide increased incentives for agencies and organisations to take seriously their obligations under the 'Data Security' principle.

28.13 There are significant differences, however, in the objectives of these provisions and the regulatory framework through which the ALRC recommends achieving these objectives. The 'Data Security' principle provides a broad framework for the protection of personal information by agencies and organisations. As with the other UPPs, the 'Data Security' principle is based on principles-based regulation. In comparison, the data breach notification provisions require agencies and organisations to take specific steps to ameliorate the harms that flow from a particular breach of data security—namely, the unauthorised acquisition of personal information. This is an example of rules-based regulation, which is better placed either in statutory provisions or in legislation.[15]

---

12 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.
13 Rec 18–2.
14 See Ch 51.
15 See Ch 4.

28.14 Due to these differences, it is not appropriate to incorporate the data breach notification provisions into the 'Data Security' principle. The ALRC recommends, however, that a note should be inserted after the 'Data Security' principle alerting agencies and organisations to their requirements under the data breach notification provisions.

Recommendation 28–1 The model Unified Privacy Principles should contain a principle called 'Data Security' that applies to agencies and organisations.

Recommendation 28–2 A note should be inserted after the 'Data Security' principle cross-referencing to the data breach notification provisions.

Prevention of misuse and loss of personal information

28.15 A central component of data security is protecting personal information from misuse and loss. The importance of measures to protect personal information from misuse and loss recently was illustrated in the United Kingdom, when Her Majesty's Revenue and Customs lost in the post the personal information of 25 million Britons, including their dates of birth, addresses, bank accounts and national insurance numbers. In particular, concerns were raised that the data lost had not been encrypted, but merely was password protected.[16]

28.16 The IPPs and the NPPs both include a requirement to protect personal information from misuse and loss. These principles, however, differ subtly. As noted above, IPP 4(a) requires agencies to ensure that a record containing personal information is protected 'by such security safeguards as is reasonable in the circumstances against unauthorised access, use, modification or disclosure and against other misuse'. An agency that does not take such steps will breach IPP 4, even if no loss, unauthorised access, use, modification or disclosure actually takes place.[17]

28.17 A number of Commonwealth documents also require agencies to adopt certain security measures. In particular, the *Protective Security Manual* (PSM) outlines minimum standards and procedures for Australian Government agencies, including requirements for: information security; personnel security; physical security; and

16 See, for example, R Blakely, 'Data 'Fiasco' Leads to Calls for Law Changes', *Times Online* (online), 20 November 2007, <http://business.timesonline.co.uk>; P Wintour, 'Lost in the Post—25 Million at Risk After Data Discs Go Missing', *The Guardian* (online), 22 November 2007, <http://politics .guardian.co.uk>.

17 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 3.

tendering and contracting.[18] Additionally, the Defence Signals Directorate (DSD) has published the *Australian Government Information and Communications Technology Security Manual* (ACSI 33), which sets out common principles for Commonwealth and state and territory agencies to protect information held on information and communications systems.[19]

28.18 NPP 4.1 requires organisations to take 'reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'. The OPC has issued guidance on how organisations should meet this requirement, including through taking steps to implement:

- physical security, such as locks, alarm systems and access limitations;
- computer and network security, such as user passwords and auditing procedures;
- communications controls, such as encryption of data; and
- personnel security, such as staff training programs.[20]

28.19 A number of national and international standards-developing bodies also are developing standards on privacy and security issues, including Standards Australia and the International Standards Organization.[21]

Submissions and consultations

28.20 The 'Data Security' principle proposed by the ALRC in DP 72 required

> an agency or organisation [to] take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.[22]

28.21 This principle mirrored the requirements currently provided in NPP 4.1. The ALRC proposed that the OPC provide guidance to agencies and organisations on how they should meet the requirement to protect personal information from misuse and loss, including through:

---

18 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 8 April 2008.

19 Australian Government Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual (ACSI 33)* (2007).

20 Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001), 1–4. The OPC has suggested similar security measures in the context of agencies: see Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998).

21 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [7.56]–[7.63].

22 Ibid, UPP 8(a).

- contracting service providers to handle personal information consistently with the proposed UPPs;

- recognising the potential benefits of, and detriments associated with, technological developments in this area, including encryption; and

- implementing adequate staff training.[23]

Criteria for data security

28.22 Several stakeholders expressed views on the proposed criteria for protecting personal information—that is, that agencies and organisations should protect personal information from 'misuse and loss and from unauthorised access, modification or disclosure'.

28.23 The OPC supported these criteria.[24] The Cyberspace Law and Policy Centre submitted, however, that 'misuse and loss' by authorised users would not necessarily encompass excessive access or accidental alteration or degradation falling short of loss. Further,

> the reference to 'unauthorised access, modification or disclosure' implies that 'loss' and 'modification' have different meanings, and it may be that neither includes the other. If so, then security need not protect against loss of data caused by unauthorised parties—which would be ridiculous.[25]

28.24 The Centre submitted, therefore, that the 'Data Security' principle be reworded to require protection against 'improper access, use, alteration, deletion, disclosure, or other misuse, by both authorised users and by other parties'.[26] The Australian Privacy Foundation supported the Centre's submission.[27]

28.25 Australia's National Computer Emergency Response Team submitted that additional provisions should be included for the security of personal information exchanged over the internet.[28]

'Reasonable steps' to protect personal information

28.26 Stakeholders supported the proposal that the OPC should provide guidance about the meaning of the term 'reasonable steps' in the context of misuse and loss of

---

23 Ibid, Proposal 25–3.
24 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
25 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
26 Ibid.
27 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
28 Australia's National Computer Emergency Response Team, *Submission PR 474*, 14 December 2007.

personal information.[29] GE Money and Microsoft Asia Pacific submitted that the factors to determine whether an agency or organisation has taken 'reasonable steps' to prevent the misuse or loss of personal information should be set out in the 'Data Security' principle, rather than being the subject of guidance.[30]

28.27 Several stakeholders suggested additional features that should be included in the OPC guidance. The Public Interest Advocacy Centre (PIAC), for example, submitted that the guidance also should address the physical security of information systems and security of computer networks and communications.[31] The Office of the Victorian Privacy Commissioner (OVPC) commented that other security developments, such as access control and audit tools, were just as important as encrypting personal information.[32] Medicare Australia suggested that the guidance should address the requirements to protect personal information disclosed to a contracted service provider.[33]

28.28 The OPC did not support providing guidance on technological developments in this area; in particular, relevant encryption standards. It submitted that:

> While the Office recognises the need for guidance in this area, it is concerned about the specialised level of expertise required to provide such guidance, along with the resource implications of continually ensuring the accuracy of guidance in a rapidly changing technological environment.[34]

28.29 The Australian Federal Police and the Department of Defence commented on the need to avoid duplication, conflict or confusion between the guidance provided by the OPC and guidance on security measures presently provided for Commonwealth agencies by other agencies, such as Australian Government Attorney-General's Department (AGD) which publishes the PSM, and the DSD which publishes the ACSI 33.[35]

---

29 Confidential, *Submission PR 570,* 13 February 2008; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559,* 15 January 2008; Australian Federal Police, *Submission PR 545,* 24 December 2007; Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Medicare Australia, *Submission PR 534,* 21 December 2007; Optus, *Submission PR 532,* 21 December 2007; Centre for Law and Genetics, *Submission PR 497,* 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; Australia Post, *Submission PR 445,* 10 December 2007; National Health and Medical Research Council, *Submission PR 397,* 7 December 2007.

30 GE Money Australia, *Submission PR 537,* 21 December 2007; Microsoft Asia Pacific, *Submission PR 463,* 12 December 2007.

31 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

32 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

33 Medicare Australia, *Submission PR 534,* 21 December 2007.

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

35 Australian Federal Police, *Submission PR 545,* 24 December 2007; Australian Government Department of Defence, *Submission PR 440,* 10 December 2007.

28.30 Privacy advocates also suggested that the requirement for agencies and organisations to take 'reasonable steps' to prevent the misuse or loss of personal information should be subject to a proportionality test—that is, that the security safeguards should be commensurate with the sensitivity of the information.[36] The Cyberspace Law and Policy Centre commented, for example, that the over-zealous application of the 'Data Security' principle could result in privacy protections which themselves become privacy infringements, and serve to impede the legitimate flow of information.[37]

ALRC's view

Criteria for data security

28.31 The criteria in the 'Data Security' principle should reflect the criteria currently provided in NPP 4.1—that is, that personal information should be protected from misuse and loss and from unauthorised access, modification or disclosure. These criteria balance the role of the 'Data Security' principle and those acts and practices that can be regulated more appropriately through other privacy principles.

28.32 Security concerns are implicit in the notion of 'misuse and loss' of personal information. These criteria, therefore, are appropriate matters for the 'Data Security' principle. In comparison, security concerns only arise where 'access', 'modification' or 'disclosure' of personal information is unauthorised. Authorised access, modification or disclosure that is, nevertheless, improper, is addressed through other privacy principles. In particular, the 'Data Quality' principle will apply to personal information that has been modified improperly. The 'Use and Disclosure' principle will apply to wrongful disclosures of personal information. Additionally, authorised access leading to unauthorised disclosure could, if sufficiently serious, engage the data breach notification provisions.[38]

28.33 The ALRC does not recommend additional data security provisions for personal information exchanged over the internet. This would be inconsistent with the ALRC's recommendation that the UPPs should be technology neutral and capable of general application.[39] The ALRC addresses issues relating to technological developments in Part B.

---

36 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. The draft Asia-Pacific Privacy Charter, for example, provides that 'security safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held': Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [22].

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

38 See Ch 51.

39 Rec 18–1.

'Reasonable steps' to protect personal information

28.34 The ALRC does not recommend expanding upon the term 'reasonable steps' in the 'Data Security' principle. Such an expansion would be inconsistent with the ALRC's recommendation that the model UPPs should be high-level principles of general application.[40] Moreover, the ALRC considers further statutory elucidation to be unnecessary given other requirements in the model UPPs—for example, the requirement for an agency or organisation to create a Privacy Policy that outlines how it proposes to handle personal information consistently with the *Privacy Act*.[41] Instead, the ALRC recommends that the OPC should develop and publish guidance on the meaning of the term 'reasonable steps' in this context. The OPC guidance will complement more specific guidance provided in certain contexts—for example, the agency-specific requirements set out in the PSM and ACSI 33.

28.35 Implementing privacy-enhancing technologies will be one of the main ways through which agencies and organisations will comply with the requirement to take steps to prevent the misuse and loss of personal information. Accordingly, the ALRC recommends that relevant technological developments, including encryption techniques, should be included in the OPC's guidance on this issue.

28.36 The ALRC acknowledges the OPC's concerns about the expertise required to provide guidance on relevant technological developments. There are a number of ways, however, in which the OPC could provide such guidance. One example is the Good Practice Note on the security of personal information issued by the United Kingdom Information Commissioner's Office. This document—without mandating or endorsing specific standards or technologies—refers readers to other sources of information, including relevant international and national standards.[42] A similar framework could be adopted by the OPC.[43]

28.37 The ALRC also recommends that the *Privacy Act* be amended to empower the Privacy Commissioner to establish expert panels at his or her discretion. In particular, the OPC could use expert panels to develop education and guidance materials relating to new and developing technologies.[44] The OPC also could consult with other bodies with expertise in the implications of technological developments for data security, for example the DSD.

---

40 See Ch 18.

41 See Ch 24.

42 United Kingdom Government Information Commissioner's Office, *Data Protection Good Practice Note—Security of Personal Information* (2007).

43 In Ch 10, the ALRC notes that mandating standards in regulations could have unintended consequences in the face of rapid technological development. The ALRC recommends, however, that in carrying out its functions under the *Privacy Act*, the OPC should have reference to the work of national and international standards bodies.

44 See Rec 46–5.

28.38 Organisational policies and procedures, such as staff training programs and the physical security of paper-based and electronic information, also will be important measures to protect personal information. The ALRC recommends, therefore, that these measures also should be addressed in the OPC guidance.

28.39 Proportionality considerations are implicit in the requirement to take 'reasonable steps'. That is, whether a particular security measure is determined to be a reasonable step for an agency or organisation to take in any given situation will depend upon factors such as the: likelihood and severity of harm threatened; sensitivity of the information; and cost of implementation. Further, where a security measure, in and of itself, could be an interference with privacy this will be a relevant factor in assessing its reasonableness.

28.40 This can be illustrated by the following example. An organisation may hold personal information electronically. To verify that an individual is entitled to access the relevant information, the organisation seeks responses to a number of questions. These questions require the individual to provide further personal information. It is logical that, when assessing whether this constitutes a 'reasonable step' to protect personal information from misuse or loss, the organisation's collection of additional personal information should be taken into account. The ALRC recommends, therefore, that proportionality considerations should be included in the OPC guidance on this issue.

Recommendation 28–3 The Office of the Privacy Commissioner should develop and publish guidance about the 'reasonable steps' agencies and organisations should take to prevent the misuse and loss of personal information. This guidance should address matters such as the:

(a) factors that should be taken into account in determining what are 'reasonable steps', including: the likelihood and severity of harm threatened; the sensitivity of the information; the cost of implementation; and any privacy infringements that could result from such data security steps; and

(b) relevant security measures, including privacy-enhancing technologies such as encryption, the security of paper-based and electronic information, and organisational policies and procedures.

Disclosure of personal information to third parties

Background

28.41 Unlike NPP 4, IPP 4 expressly obliges a record-keeper to take reasonable steps to prevent unauthorised use or disclosure of personal information contained in a record

where the record is given 'to a person in connection with the provision of a service to the record-keeper'.[45] In addition, s 95B of the *Privacy Act* requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a service provider does not do an act or engage in a practice that would breach the IPPs.[46] This raises the question of whether the 'Data Security' principle should require organisations, as well as agencies, to ensure the protection of personal information they disclose to contractors.[47]

28.42 A potential advantage of making specific provision in this area is that it would overcome some of the problems that arise where an organisation engages in outsourcing—for example, where an organisation subcontracts to an entity that is not covered by the *Privacy Act*. The OPC has responded to the problem of outsourcing by issuing guidance, stating that 'where there is a particularly close relationship between an organisation and a contractor it may mean that the actions of the contractor could be treated as having been done by the organisation'.[48] In the specific context of an organisation that contracts with an entity that is subject to the small business exemption, the OPC stated:

> If an organisation is contracting with a business that is not covered by the *Privacy Act* it would be advisable to encourage the contractor to opt in to being covered … One way of doing this would be to make opting in a condition of the contract.
>
> Another less effective option would be for the organisation to have terms and conditions in the contract. These would bind the contractor to taking steps necessary to protect the personal information it holds that would be equivalent to the steps required by the NPPs.[49]

28.43 In 2005, the OPC recommended that the Australian Government consider amending NPP 4 to require organisations to ensure the protection of personal information they disclose to contractors.[50]

Submissions and consultations

28.44 In DP 72, the ALRC proposed that the 'Data Security' principle should require an agency or organisation

> to take reasonable steps to ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to

---

45 *Privacy Act 1988* (Cth) s 18G imposes similar data security obligations on credit reporting agencies and credit providers in respect of credit files and reports given to persons in connection with the provision of a service to those agencies or providers. Credit reporting is discussed in detail in Part G.

46 Section 95B is discussed in detail in Ch 14.

47 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–17.

48 Office of the Federal Privacy Commissioner, *Contractors*, Information Sheet 8 (2001).

49 Ibid. Note, however, that the ALRC recommends removing the small business exemption from the Act: see Ch 39.

50 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 54. See also rec 56, which states that the OPC should issue guidelines to clarify that businesses, which give personal information to contractors, should impose contractual obligations on any contractors to take reasonable steps to protect the information.

> the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.[51]

28.45 A large number of stakeholders supported the proposed expansion of the 'Data Security' principle.[52] Optus noted, for example, that 'obligations on contractors, as well as organisations, improve accountability and serves to strengthen Australia's privacy regime'.[53] PIAC commented that this obligation, in addition to the proposal to remove the small business exemption, would ensure that there are very few situations where contractors would be able to operate without being subject to privacy principles.[54] The Australian Bankers' Association (ABA) supported the proposal, provided it operated independently of the 'Cross-border Data Flows' principle.[55] Suncorp-Metway supported the proposal subject to not having to alter any contracts retrospectively.[56]

28.46 Some stakeholders suggested that limiting the obligation to contractors or disclosure 'otherwise in connection with the provision of a service to the agency or organisation' was unnecessarily narrow.[57] The Cyberspace Law and Policy Centre, for example, submitted that the obligation should apply to all personal information that an agency or organisation discloses to a third person.[58] Privacy advocates also suggested that an agency or organisation should take steps to require third parties to handle personal information in accordance with privacy requirements other than the 'Use and Disclosure' principle, including: the remaining obligations in the 'Data Security' principle;[59] the 'Notification' principle;[60] the 'Data Quality' principle;[61] and the

---

51 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 25–2.

52 Australian Government Centrelink, *Submission PR 555,* 21 December 2007; 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; Medicare Australia, *Submission PR 534,* 21 December 2007; Optus, *Submission PR 532,* 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; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; National Health and Medical Research Council, *Submission PR 397,* 7 December 2007.

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

54 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

55 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008.

56 Suncorp-Metway Ltd, *Submission PR 525,* 21 December 2007.

57 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Smartnet, *Submission PR 457,* 11 December 2007.

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

59 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

60 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

61 Ibid.

'Cross-border Data Flows' principle.[62] The Australian Privacy Foundation suggested that third party recipients should be required to observe all relevant UPPs in relation to that information.[63] Smartnet submitted that the principle should extend so that the

> initial collecting organisation remain[s] accountable for the use and protection of all information it collects, even when that information has been transferred to another party.[64]

28.47 Several organisations did not support the ALRC's proposal.[65] The Recruitment and Consulting Services Association Australia and New Zealand submitted that the principle of individual responsibility is a more effective and less costly way of ensuring good privacy compliance.[66] GE Money was concerned that

> the privacy regime will not sufficiently recognise the extent to which organisations outsource a wide variety of functions and the extent to which the organisation cannot provide products and services unless these disclosures take place.[67]

28.48 Two stakeholders also sought clarification on what would be required for agencies and organisations to ensure that personal information disclosed to that service provider is handled in accordance with the UPPs.[68] ANZ submitted that, provided a third party has agreed to undertake 'reasonable steps' to protect personal information, this should satisfy the proposed requirement. ANZ noted:

> As an overriding principle, ANZ would not enter into a contractual arrangement with a third party if it believed the party did not have adequate information security processes in place.[69]

28.49 In comparison, the Cyberspace Law and Policy Centre submitted that compliance with the principle should include the recipient demonstrating a commitment to comply with the relevant privacy obligations, for example through a privacy policy.[70]

ALRC's view

28.50 The ALRC does not recommend that a requirement be included in the 'Data Security' principle for agencies and organisations to protect information disclosed to third parties. Even in the absence of such a requirement, agencies remain subject to the

---

62 Ibid.
63 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
64 Smartnet, *Submission PR 457*, 11 December 2007.
65 GE Money Australia, *Submission PR 537*, 21 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.
66 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.
67 GE Money Australia, *Submission PR 537*, 21 December 2007.
68 Medicare Australia, *Submission PR 534*, 21 December 2007; ANZ, *Submission PR 467*, 13 December 2007.
69 ANZ, *Submission PR 467*, 13 December 2007.
70 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

requirements in s 95B of the *Privacy Act*—that is, the agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles. There is no need for a change to the current law.

28.51 This position assumes the implementation of other recommendations in this Report—in particular, the removal of the small business exemption[71] and the recommended changes to the 'Cross-border Data Flows' principle.[72] Provided these recommendations are implemented, there will be few, if any, situations where a contracted party will not be under an obligation to comply with the *Privacy Act*. Accordingly, a requirement for contracting organisations to ensure that personal information disclosed in accordance with a contract retains privacy protections will be largely redundant.

28.52 If the above recommendations are not implemented, however, then a requirement for organisations to take steps to protect information disclosed to a third party pursuant to a contract, or otherwise in connection with the provision of a service, will be an integral component of the *Privacy Act*. This could be included in the 'Data Security' principle, as proposed in DP 72, or as a separate 'contractors' provision, similar to the s 95B requirements.

Information destruction and retention requirements

Background

28.53 Sometimes privacy law requires an agency or organisation that has collected personal information to destroy, delete or de-identify that information after a set period of time or in certain circumstances. This requirement may arise where, for example, an organisation has collected personal information for the specific purpose of identifying an individual. When the identification process has been completed, the organisation may no longer have a lawful reason to hold the personal information. Accordingly, destruction or de-identification of the information may be the most effective means of ensuring that the individual's information is not subsequently misused or disclosed without authorisation.

71 The small business exemption is discussed in Ch 39.
72 The 'Cross-Border Data Flows' principle is discussed in Ch 31.

28.54 The NPPs require an organisation to

> take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under [the 'Use and Disclosure' principle].[73]

28.55 No equivalent obligation applies to agencies under the IPPs.[74] A number of other jurisdictions, however, impose such a requirement on government agencies. For example, Canadian government institutions must dispose of personal information in their control in accordance with regulations under the *Privacy Act 1985* (Canada) and rules promulgated by the responsible minister.[75] German privacy law also requires public bodies to erase personal data in certain circumstances.[76] Similarly, some state and territory laws require government bodies to destroy or permanently de-identify personal information when it is no longer needed.[77]

28.56 Conversely, privacy and other laws may require an agency or organisation to *retain* personal information for a minimum period of time. The requirement to retain personal information arises frequently in the context of health care and research. For example, the 'data security and data retention' principle in Victorian health privacy law limits the circumstances in which a health service provider can delete information, and sets out certain procedures to be followed where deletion is allowed.[78]

28.57 Requirements to retain personal information also arise under public sector archives legislation.[79] The *Archives Act 1983* (Cth) prohibits the destruction of Commonwealth records without the permission of the National Archives of Australia (National Archives), subject to certain exceptions. These exceptions include where destruction is 'required by any law' or is in accordance with a 'normal administrative practice'.[80]

28.58 The Management Advisory Committee[81] has issued the report, *Note for File: A Report on Record-Keeping in the Australian Public Service*, which sets out the Australian Government's record-keeping obligations. This document provides that

---

73 *Privacy Act 1988* (Cth) sch 3, NPP 4.2. In the recommendation below and in the 'Data Security' principle, the ALRC avoids using the term 'de-identify' and instead uses the term 'render non-identifiable'. This change in terminology reflects the position discussed in Ch 6 and later in this chapter.

74 Section 18F of the *Privacy Act*, however, requires credit providers and credit reporting agencies to delete certain personal information in accordance with prescriptive timeframes.

75 *Privacy Act* RS 1985, c P-21 (Canada) s 6(3).

76 *Federal Data Protection Act 1990* (Germany) s 20(2).

77 See *Information Privacy Act 2000* (Vic) sch 1, IPP 4.2; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 4(2); *Information Act 2002* (NT) sch 2, IPP 4.2.

78 See *Health Records Act 2001* (Vic) sch 1, Health Privacy Principles 4.2, 4.3. These procedures involve the making of a written note of the person to whom the deleted information related, the period covered by the information and the date of deletion. This is discussed further in Part H.

79 See *Archives Act 1983* (Cth).

80 Ibid s 24.

81 The Management Advisory Committee is a forum of Secretaries and Agency Heads established under the *Public Service Act 1999* (Cth) to advise the Australian Government on matters relating to the management of the Australian Public Service.

only a small proportion of Commonwealth records need to be retained by the National Archives, including 'significant policy documents, and records of significant decisions'.[82] Documents outside this class may be disposed of once there is no longer a business need for their retention. For example:

- conversational, personal or other unimportant emails which record no significant information, action or decision
- most draft documents and working papers which do not record a significant change of policy/direction
- informal notes/notepads/diaries, where any significant information has been properly transferred to the agency's corporate recordkeeping systems
- superfluous copies of any Commonwealth record.[83]

Options for reform

28.59 The ALRC has considered two reforms directed towards clarifying what is required of a regulated entity in order to fulfil its data destruction requirements:

- changing the terminology used in the data destruction principle; and
- imposing more specific requirements for how personal information should be 'destroyed'.

28.60 The ALRC also has considered possible changes to the scope of data destruction requirements, including:

- applying the data destruction principle to agencies;
- modifying the permitted reasons for retaining personal information; and
- providing individuals with the right to request the destruction of personal information.

Terminology for data destruction

28.61 As noted above, currently the NPPs require organisations to 'destroy or permanently de-identify' personal information where it is no longer needed. Stakeholders have suggested that the term 'de-identification' is not sufficiently clear in the context of the *Privacy Act*.[84] The ALRC has examined the appropriate terminology

---

82 Australian Government Management Advisory Committee, *Note for File: A Report on Recordkeeping in the Australian Public Service* (2007), 3.

83 Ibid, 16.

84 See, for example, CSIRO, *Submission PR 176*, 6 February 2007. See also, in the context of research, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

for any data destruction requirement, including the approach that should be taken to information that falls outside the definition of 'personal information' for the purposes of the *Privacy Act*. This issue is discussed in Chapter 6.

28.62 In DP 72, the ALRC suggested that the term 'permanently de-identify'—both in the context of the 'Data Security' principle and more broadly in the *Privacy Act*—should be replaced with the alternative term 'render non-identifiable'.[85] A few stakeholders supported this change in terminology in the context of the data destruction requirement.[86] Two stakeholders submitted, however, that the terms 'destroy' and 'render non-identifiable' should be defined in the *Privacy Act*.[87]

ALRC's view

28.63 The term 'render non-identifiable' should be used in the 'Data Security' principle, rather than the term 'permanently de-identify'. This makes it clear that compliance with a data destruction requirement includes taking steps to prevent future re-identification of data.

28.64 Consider the following hypothetical example. An organisation holds property-related documents containing personal information about one of its customers, X. When X ceases to be a customer, the organisation, in the absence of any other legal requirement, no longer has a lawful purpose for holding these documents, and therefore is subject to a data destruction requirement. If the organisation merely blacks out X's name wherever it appears, arguably the documents have been permanently de-identified. This will not necessarily preclude the documents from later being re-identified, however, if a person is able to match the information in these documents with other publicly available information, such as government land title information. On the other hand, an obligation to render the information non-identifiable would require the organisation to take additional steps to ensure that the information in the documents cannot be matched easily with other available data to allow the documents to be re-identified.

28.65 In Chapter 6, the ALRC concludes that it is unnecessary to include definitions of 're-identifiable data' and 'non-identifiable data' in the *Privacy Act*. Rather, the relevant

---

Submissions to this effect also were made to the OPC review of the private sector provisions: 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; Australian Institute of Health and Welfare, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 23 December 2004; 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.

85 This change in terminology is discussed in DP 72: Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Chs 3, 25 and 58.

86 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

87 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

question is whether information is about 'an identified or reasonably identifiable individual'. This decision will always be contextual and will have to be considered on a case-by-case basis.

Manner of destroying or rendering non-identifiable personal information

Background

28.66 A further issue is whether requirements should be imposed—either in law or by the OPC—stipulating what an entity needs to do to destroy or render non-identifiable personal information. For example, in the context of deleting digital records, the Victorian Society for Computers and the Law has noted that:

> [E]specially in the case of larger organisations, it may be practically impossible to guarantee the complete destruction of particular information, or if it is possible, the destruction process may be unreasonably costly and burdensome. The practical effect is that organisations requested to delete information may be encouraged to disregard such requests, to make only cursory and incomplete attempts to delete information, or to pass on the costs of deletion to consumers.[88]

28.67 One model for providing such guidance is the *Fair and Accurate Credit Transactions Act 2003* (US), which requires companies that handle consumer reports to destroy information in accordance with regulations issued by the relevant regulatory agency.[89] The Final Rule issued by the Federal Trade Commission, for example, requires persons to 'properly dispose of [consumer information] by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal'.[90] Reasonable measures include:

- implementing and monitoring compliance with policies and procedures that require the burning, pulverizing or shredding of papers containing consumer information so that the information cannot practically be read or reconstructed;
- implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practically be read or reconstructed;
- after due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of

88 Victorian Society for Computers and the Law Inc, *Submission PR 137*, 22 January 2007.
89 *Fair and Accurate Credit Transactions Act 2003* (United States) § 628.
90 United States Government Federal Trade Commission, *Disposal of Consumer Report Information and Records; Final Rule* (2005), § 682.3 (a).

material, specifically identified as consumer information, in a manner consistent with the rule.[91]

28.68 Alternatively, regulated entities could be required to destroy or render non-identifiable personal information in compliance with an industry standard. For example, the National Association for Information Destruction (NAID) Certification Program sets out minimum standards for information destruction services, including security, employee hiring and screening, operational destruction programs and insurance.[92]

Submissions and consultations

28.69 In DP 72, the ALRC suggested that guidance should be developed and published by the OPC on the requirement to destroy or render non-identifiable personal information.[93] The majority of stakeholders that commented on this issue supported the ALRC's proposal.[94]

28.70 Other stakeholders provided qualified support. The NHMRC noted the need for some health information and non-health genetic information to be re-identified in the future.[95] NAID suggested that there should be clear guidance in Australian privacy laws to require businesses that have privacy obligations for secure information destruction to do so in accordance with an industry standard.[96] Optus suggested that, in formulating this guidance, the OPC should have regard to the practical implications of these activities and should consult broadly with industry experts on these matters.[97]

ALRC's view

28.71 The requirement to destroy or render non-identifiable personal information has caused considerable confusion. The ALRC recommends, below, that the OPC should provide guidance about the responsibilities agencies and organisations have under the 'Data Security' principle. This should include guidance on the manner in which personal information should be destroyed or rendered non-identifiable. This guidance should address both paper-based records and electronic media. It also may be useful for this guidance to refer to relevant standards for information destruction; for example, the requirements of the NAID Certification Program.

---

91 Ibid, § 82.3 (b).

92 National Association for Information Destruction Inc, *NAID Certification Program—January 2008* (2008); National Association for Information Destruction Inc, *NAID Certification Program for Information Destruction Operations* <www.naidonline.org> at 18 April 2008.

93 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 25–6.

94 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Medicare Australia, *Submission PR 534*, 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.

95 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

96 National Association for Information Destruction (Australasia), *Submission PR 483*, 17 December 2007.

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

Extending the data destruction requirement to agencies?

28.72 As noted above, the *Privacy Act* currently imposes a requirement to destroy personal information only to organisations. In DP 72, the ALRC proposed that the 'Data Security' principle should impose a data destruction requirement on both agencies and organisations—that is, they should be required to destroy or render non-identifiable personal information, where it is no longer necessary for a purpose permitted by the UPPs.[98]

Submissions and consultations

28.73 A number of government and non-government stakeholders supported applying a 'data destruction' requirement to agencies.[99] As one stakeholder commented:

> The single greatest protection for personal information against unexpected and unwelcome secondary uses, and 'function creep' is to delete or de-identify it. If it no longer exists in identifiable form, it can no longer pose a risk to privacy.[100]

28.74 The Queensland Government, however, did not support applying a uniform requirement to destroy or render non-identifiable personal information to agencies and organisations. It noted:

> to suggest that agencies could simply destroy personal information either at the point of reception or when it is deemed no longer necessary for the purpose for which it was collected disregards that governmental decisions and actions must be transparent.[101]

28.75 National Archives suggested that, because of requirements under the *Archives Act*, records of Commonwealth agencies should be excepted from any requirement under the UPPs to destroy or render non-identifiable personal information.[102] The

---

98 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 25–4.

99 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 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; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

100 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

101 Queensland Government, *Submission PR 490*, 19 December 2007.

102 National Archives of Australia, *Submission PR 414*, 7 December 2007.

Australian Federal Police also submitted that any data destruction decisions should be left to the agency and legislation such as the *Archives Act*.[103]

28.76 A number of stakeholders—while not opposing the extension of a data destruction requirement to agencies—were concerned about the potential damage that could be caused if records are destroyed prematurely.[104] The South Australian Government noted that destroying information, or rendering it non-identifiable, can have a negative effect. Destruction of juvenile justice records from the 1970s, for example, has limited the work of the current South Australian Commission of Inquiry into Children in State Care. It also noted a number of situations where the failure to destroy or render information non-identifiable permitted positive action to be taken. For example:

- retention of records from the former South Australian Protector of Aborigines and adoption records has assisted in the process of reconnecting members of the Stolen Generation with their families
- adoption, immigration and social welfare records have assisted with the reunification of child migrants with family members
- workers compensation cases, such as those for asbestosis have been successfully concluded because of the retention of a range of employment and health records
- internationally, a range of reconstruction issues post-WWII and post-'Cold War' have been assisted by the retention of records from the former governments.[105]

28.77 PIAC noted that much of its work in the 'Stolen Wages' project would not have been possible if the personal information of claimants had been destroyed or rendered non-identifiable by government agencies.[106] The Human Rights and Equal Opportunity Commission noted that the *Bringing Them Home* Report recommended

> that no records relating to Indigenous individual, families or communities or to any children, Indigenous or otherwise, removed from their families for any reason, whether held by government or non-government agencies, be destroyed.[107]

---

103 Australian Federal Police, *Submission PR 545*, 24 December 2007.

104 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

105 Government of South Australia, *Submission PR 565*, 29 January 2008.

106 The Stolen Wages project involved the investigation of claims by Indigenous clients who were denied access to wages, allowances and pensions held on trust by the Aborigines Welfare Board and subsequently the NSW Government.

107 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007, referring to Human Rights and Equal Opportunity Commission, *Bringing Them Home: Report of the National Inquiry into the Separation of Aboriginal and Torres Strait Islander Children from their Families* (1997).

28.78 Australian Government Centrelink and Suncorp-Metway Ltd also commented that compliance with this proposal could be a potentially onerous administrative burden on agencies and organisations.[108]

ALRC's view

28.79 Destroying, or rendering non-identifiable, personal information provides an important layer of privacy protection by removing the possibility of future misuse of, or unauthorised access to, that information. These benefits apply equally to personal information held by agencies and organisations. Accordingly, there are compelling policy reasons why a data destruction requirement should apply to agencies as well as organisations.

28.80 Concerns have been raised by a number of stakeholders—in particular, agencies—about the potential for a data destruction requirement to conflict with other requirements for agencies to retain information. These concerns can be accommodated adequately by wording carefully the permitted reasons for retention of personal information. This issue is considered below.

Permitted reasons for retaining personal information

28.81 NPP 4.2 requires organisations to destroy personal information 'if it is no longer needed for any purpose for which the information may be used or disclosed under [the 'Use and Disclosure' principle]'. The 'Data Security' principle that was proposed in DP 72 included similar reasons for retention—that is, that personal information may be retained if it is 'needed for any purpose permitted by the UPPs'.

Submissions and consultations

28.82 A number of stakeholders submitted that it is unlikely that the permitted reasons for retention of personal information that the ALRC proposed would resolve potential conflicts with other legal obligations to retain information.[109] The AGD advised that the 'Data Security' principle would need to accommodate situations where an agency's enabling legislation requires it to retain personal information.[110] GE Money was concerned that the ALRC's formulation might not cover an organisation that keeps the information for the purpose of dispute resolution.[111]

---

108 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

109 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; National Archives of Australia, *Submission PR 414*, 7 December 2007.

110 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

111 GE Money Australia, *Submission PR 537*, 21 December 2007.

28.83 The National Archives commented that, without suitable qualifications, the proposed 'data destruction' requirement could undermine the requirement in the *Archives Act* to obtain the permission of Archives before destroying or altering personal information contained in Commonwealth records.

> Such a gap may lead to the unregulated destruction of public records containing personal information through zealous interpretation, or deliberate misuse to avoid accounting for government actions involving individuals.[112]

28.84 Some stakeholders suggested that there should be an exception from the data destruction requirement for health records.[113] The National Health and Medical Research Council (NHMRC), for example, advised that the *Australian Code for the Responsible Conduct of Research* recommends a minimum retention period for research data of five years from the date of publication. Longer retention periods are provided for particular areas of research. For example, clinical trial data should be retained for a minimum of 15 years. For areas such as gene therapy, research data must be retained permanently.[114]

28.85 The Department of Health and Ageing submitted that the requirement for an agency or organisation to destroy or render non-identifiable personal information should take into account primary and secondary purposes. This could be relevant particularly to genetic information and samples.[115]

28.86 Other stakeholders submitted that the purpose for which personal information may be retained under the proposed 'data destruction' requirement—that is, where the information is needed for any purpose permitted by the UPPs—should be more stringent.[116] The Cyberspace Law and Policy Centre and the Australian Privacy Foundation, for example, suggested that personal information should be retained only for a secondary purpose for which it has already legitimately been used, or where there is express legal authority for retention.[117] One stakeholder also submitted that the 'data destruction' requirement should provide a maximum time frame for retention of personal information.[118]

---

112 National Archives of Australia, *Submission PR 414*, 7 December 2007.

113 Medicare Australia, *Submission PR 534*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

114 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

115 Confidential, *Submission PR 570*, 13 February 2008.

116 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

117 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

118 S Hawkins, *Submission PR 382*, 6 December 2007.

ALRC's view

28.87 The data destruction requirement included in the 'Data Security' principle must be worded so as to accommodate the various reasons why agencies and organisations may need to retain personal information. These include, for example, where the information is still necessary for its primary purpose of collection or where destruction could conflict with a legal obligation to retain the information.

28.88 This can be achieved by including two limbs for the retention of personal information. First, personal information should be destroyed or rendered non-identifiable 'if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs'. This limb is equivalent to the current formulation in NPP 4.

28.89 Secondly, the retention of personal information should be permitted expressly where retention is required or authorised by or under law.[119] In particular, this exception is directed towards the potential conflict between a data destruction requirement and agencies' archiving obligations. It also will address concerns raised by stakeholders about: the potential for a data destruction requirement to conflict with a relevant requirement under an agency's enabling legislation; and the need for an agency or organisation to retain personal information in the event of future litigation. In Chapter 16, the ALRC discusses the scope of exceptions to the *Privacy Act* for acts and practices that are 'required or authorised by or under law'. It is appropriate that (where relevant) the acts and practices considered in Chapter 16 should be excepted from the recommended data destruction requirement.

28.90 Even with the recommended exception for acts and practices that are 'required or authorised by or under law', the interaction between the data destruction requirement in the *Privacy Act* and the retention provisions of the *Archives Act* still may be ambiguous. In particular, s 24(2) of the *Archives Act* provides an exception from the requirement not to destroy, or otherwise dispose of, a Commonwealth record where destruction is 'required by law'. It is unclear whether the obligation to comply with the destruction requirements in the 'Data Security' principle are 'required by law' within the context of s 24(2) of the *Archives Act*.

28.91 Agencies' responsibilities under the *Archives Act* should take precedence over the data destruction requirement in the 'Data Security' principle. In order to make this policy clear, the ALRC recommends that the 'Data Security' principle provide that the obligation to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act*. The finer detail of drafting and decisions about whether the provision is best placed in the 'Data Security' principle or in the *Archives Act* are matters for the Australian Government to resolve, with the assistance of the Office of Parliamentary Counsel.

---

119 The term 'required or authorised by or under law' is discussed in Ch 16.

28.92 The application of the recommended data destruction requirement can be illustrated using the example of an agency that collects personal information for the purpose of a clinical trial. The agency can retain the information for as long as it is needed for the primary purpose of collection—that is, the clinical trial. The *Australian Code for the Responsible Conduct of Research* provides that, for most clinical trials, information should be retained for a minimum of 15 years.[120] This will be relevant to determining whether the information is still 'needed' for the clinical trial. After this period of time, the agency should destroy the information or render it non-identifiable, unless:

- it is necessary for a secondary purpose for which it can be used or disclosed under the model UPPs. This could include, for example, inclusion in a properly constituted research database; or

- retention is required or authorised by or under law. This could include, for example, where the information is subject to archiving obligations.

28.93 The application of the recommended data destruction requirement is sufficiently flexible to accommodate the various types of personal information that is held by agencies and organisations. The ALRC acknowledges that there often will be a need to retain health information for a longer period of time than other personal information. This may include follow-up on adverse events associated with particular treatments or research projects. This will be a factor in whether the information is still 'needed'. Accordingly, there is no need for a specific exception for health information.

Recommendation 28–4 (a) The 'Data Security' principle should require an agency or organisation to take reasonable steps to destroy or render non-identifiable personal information if:

(i) it is no longer needed for any purpose for which it can be used or disclosed under the model Unified Privacy Principles; and

(ii) retention is not required or authorised by or under law.

(b) The obligation to destroy or render non-identifiable personal information is not 'required by law' for the purposes of s 24 of the *Archives Act 1983* (Cth).

120 National Health and Medical Research Council and Australian Research Council, *Australian Code for the Responsible Conduct of Research* (2007), [2.1].

General right to destruction of personal information

28.94 A further issue that arises in relation to data destruction is whether an individual should have the right to request that an agency or organisation destroy personal information that relates to him or her and, if so, in what circumstances or upon what conditions should such a right be exercisable.[121]

28.95 Stakeholders have generally opposed amending the privacy principles to give individuals the right to request that agencies and organisations destroy their personal information.[122] Some were concerned that such a requirement would be too blunt an instrument, because it would not allow agencies and organisations to deal with the information otherwise than by destruction, even if some other method would be more appropriate.[123] Moreover, some stakeholders suggested that individuals' rights of access and correction adequately address the underlying problem.[124]

ALRC's view

28.96 The ALRC does not support giving an individual a general right to require that an agency or organisation destroy personal information it holds about the individual. Such an amendment could promote unnecessary rigidity by encouraging personal information to be destroyed even where another method of dealing with the information would be more appropriate—for example, where rendering non-identifiable personal information could satisfy the privacy rights of an individual while concurrently allowing organisations to evaluate the effectiveness of a program or activity to which the information relates. Such an amendment also may conflict with retention and destruction obligations set out in other legislation, for example, archives legislation.

OPC guidance

28.97 The application of a data destruction requirement is not always self-evident. In particular, uncertainty may arise about when it is appropriate to destroy or render non-identifiable personal information. As noted above, confusion also arises about the manner in which information should be destroyed or rendered non-identifiable.

---

121 See, eg, Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–19.

122 Optus, *Submission PR 532,* 21 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

123 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

124 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007. The 'Access and Correction' principle is discussed in Ch 29.

28.98 In DP 72, the ALRC proposed that the OPC provide guidance as to when it is appropriate to destroy or render non-identifiable personal information that is no longer needed.[125] The ALRC suggested that this guidance could address situations where destruction of personal information would be inappropriate—for example, if the personal information may later be needed for the purposes of litigation.

28.99 A number of stakeholders supported the provision of OPC guidance on the data destruction requirements.[126] Some stakeholders expressed particular support for certain aspects of the proposed OPC guidance, including: personal information that forms part of a historical record;[127] and the interaction between the data destruction requirement and legislative records retention requirements.[128]

28.100 The ABA submitted, however, that the OPC is not in a position to determine when an organisation 'needs' to retain personal information.[129] Similarly, GE Money submitted that

> the guidance suggested in this proposal is not primarily concerned with matters of privacy law … Different organisations in different industries are faced with a large range of record retention obligations under many pieces of legislation. Organisations must consider these sometimes complex and overlapping obligations and form and implement compliant record retention policies that they consider to be compliant with all relevant legislation.[130]

28.101 Some stakeholders commented on the role for OPC guidance in addressing the relative merits of destruction and de-identification of personal information.[131] The Cyberspace Law and Policy Centre, for example, submitted that destruction sometimes could be preferable to de-identification, such as where retaining non-identifiable data could lead to statistical inferences being drawn about a group of people.[132] In comparison, the OVPC submitted that—in light of the potential statistical and research value of information—information generally should be retained in a de-identified

---

125 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 25–5.

126 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Confidential, *Submission PR 519*, 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; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

127 National Archives of Australia, *Submission PR 414*, 7 December 2007.

128 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

129 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

130 GE Money Australia, *Submission PR 537*, 21 December 2007.

131 Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; National Archives of Australia, *Submission PR 414*, 7 December 2007.

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

form.[133] Optus submitted that the OPC should ensure that the obligation on agencies and organisations to destroy or render non-identifiable information is applied flexibly.[134]

28.102 The OPC noted that guidance on the relationship between the UPPs and legislative records retention requirements would need to be developed in collaboration with agencies having expertise in those other requirements.[135] Other stakeholders also noted the need for further consultation by the OPC with: consumer groups, privacy advocates and community legal centres;[136] National Archives;[137] and state and territory privacy commissioners.[138]

ALRC's view

28.103 The OPC should provide guidance on when it is appropriate to destroy or render non-identifiable personal information that 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. In particular, guidance usefully could address when it is appropriate to destroy or render non-identifiable personal information that forms part of a historical record and personal information that may be needed for the purpose of future dispute resolution. OPC guidance also could clarify the interaction between the data destruction requirements and legislative records retention requirements.

28.104 The decision whether an agency or organisation destroys personal information or, in the alternative, renders the information non-identifiable is a decision for that agency or organisation. Provided the information is no longer about an individual who is 'identified or reasonably identifiable', it is outside the ambit of the *Privacy Act*.[139] Where the information is rendered non-identifiable, rather than destroyed, use of the information for the research proposal will be governed by broader principles of research ethics and, where appropriate, review by a Human Research Ethics Committee.[140]

---

133 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
134 Optus, *Submission PR 532*, 21 December 2007.
135 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
136 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
137 National Archives of Australia, *Submission PR 414*, 7 December 2007.
138 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
139 The definition of personal information is discussed in Ch 6.
140 The relationship between privacy laws and research is discussed in Chs 64–66.

Recommendation 28–5 The Office of the Privacy Commissioner should develop and publish guidance about the destruction of personal information, or rendering such information non-identifiable. This guidance should address matters such as:

(a) when it is appropriate to destroy or render non-identifiable personal information, including personal information that:

(i) forms part of a historical record; and

(ii) may need to be preserved, in some form, for the purpose of future dispute resolution;

(b) the interaction between the data destruction requirements and legislative records retention requirements; and

(c) the manner in which personal information should be destroyed or rendered non-identifiable.

Summary of 'Data Security' principle

28.105 The eighth principle in the model UPPs should be called 'Data Security'. It may be summarised as follows.

UPP 8. Data Security

8.1 An agency or organisation must take reasonable steps to:

(a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure; and

(b) 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.

8.2 The requirement to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act 1983* (Cth).

Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.

29. Access and Correction

Contents

Introduction

29.1 Australian law sets out rights and obligations in relation to an individual's access to, and correction of, personal information held by an agency or organisation. The access and correction provisions generally reflect the 'Individual Participation Principle' in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines).[1] They also reflect a core principle in the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) (EU Directive)—namely, that

> the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her.[2]

29.2 The regimes governing access to, and correction of, personal information currently differ as between agencies and organisations. Access to, and correction of, personal information held by agencies is regulated by provisions of the *Freedom of Information Act 1982* (Cth) (FOI Act) and the Information Privacy Principles (IPPs) of the *Privacy Act 1988* (Cth)—specifically, IPPs 6 and 7. Access to, and correction of, personal information held by organisations is governed by the National Privacy Principles (NPPs) of the *Privacy Act*.

29.3 In this chapter, the ALRC recommends that the model Unified Privacy Principles (UPPs)[3] should contain an 'Access and Correction' principle that sets out a predominantly unified scheme for access to, and correction of, personal information held by agencies and organisations. Some differences have been recommended, however, in the access and correction regimes for agencies, as distinct from organisations. These differences primarily concern the exceptions to the obligation on agencies and organisations to provide individuals with access to their personal information.

29.4 The ALRC also recommends that new obligations be imposed on agencies and organisations responding to a request for access, including that an agency or organisation should respond to a request for access in a timely manner and, where reasonable, provide access in the form requested by the individual. Finally, the ALRC recommends that, where personal information held by an agency or organisation is

---

1 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 13.

2 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 12.

3 The ALRC recommends that the IPPs and NPPs should be consolidated into a single set of privacy principles, the UPPs, which generally would be applicable to agencies and organisations: see Rec 18–2.

shown to be incorrect, that agency or organisation should be required, in certain circumstances, to notify third parties to whom the information has been disclosed.

The 'Access and Correction' principle

Background

Agencies

29.5 As noted above, access to, and correction of, personal information held by agencies is regulated by a combination of provisions of the FOI Act and IPPs 6 and 7. IPP 6 provides that an individual is entitled to access a record containing his or her personal information, where it is in the possession or control of a record-keeper, except to the extent that the record-keeper is required or authorised to refuse access under any law of the Commonwealth that provides for access by persons to documents. Accordingly, IPP 6 provides individuals with the same right of access to information as is available under the FOI Act.[4]

29.6 IPP 7 provides that a record-keeper who has possession or control of a record containing personal information must take such steps, if any, as are reasonable to ensure that the record is accurate and is relevant, up-to-date, complete and not misleading. If the record-keeper is not willing to amend a record as requested by an individual, and is not required to amend it by a decision or recommendation under applicable Commonwealth law, the record-keeper must, if requested by the individual concerned, take reasonable steps to attach to the record any statement by the individual of the correction, deletion or addition sought.

Organisations

29.7 Access to, and correction of, personal information held by organisations currently is governed by NPP 6. NPP 6.1 provides that, if an organisation holds personal information about an individual, generally it must provide the individual with access to the information. It then lists a number of situations where access can be denied or limited. Where an organisation is not required to provide access under NPP 6.1, it must consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.[5] NPP 6.2 permits an organisation to give an individual an explanation for a decision, rather than direct access to personal information, where providing direct access would reveal evaluative

---

4 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 13. Another law of the Commonwealth that provides access by persons to documents is the *Archives Act 1983* (Cth).

5 *Privacy Act 1988* (Cth) sch 3, NPP 6.3. Compare also s 18H, which provides that, in certain circumstances, an individual's rights of access to credit information files and credit reports may be exercised by another person authorised in writing by the individual.

information generated within the organisation in connection with a commercially sensitive decision-making process.

29.8 NPP 6.5 provides that an organisation must take reasonable steps to correct personal information that it holds, if the individual to whom the information relates is able to establish that it is not accurate, complete and up-to-date. If the individual and the organisation disagree about the accuracy of the information, and the individual asks the organisation to associate with the information a statement claiming the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to comply with the request.[6] Finally, NPP 6.7 provides that an organisation must provide reasons for denial of access or a refusal to correct personal information.

A unified principle?

29.9 As noted above, different regimes currently apply to access to, and correction of, personal information held by agencies and organisations. In particular, these differences accommodate the overlap between the *Privacy Act* and the FOI Act, where personal information is held by agencies.

29.10 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC expressed the preliminary view that different access and correction regimes should continue to apply to agencies and organisations. The proposed regimes were as follows:

- provisions in a separate Part of the *Privacy Act* dealing with access to, and correction of, personal information held by agencies;[7] and

- an 'Access and Correction' principle in the proposed UPPs dealing with access to, and correction of, personal information held by organisations.[8]

ALRC's view

29.11 As discussed in Chapter 15, the 'Access and Correction' principle can be formulated to apply both to agencies and organisations. This is consistent with the ALRC's recommendation that, unless there is a sound policy reason to the contrary, the privacy principles should apply equally to agencies and organisations.[9]

29.12 Differences between the current access and correction obligations on agencies and organisations are discussed in later sections of this chapter. Where there is a good

6 Ibid sch 3, NPP 6.6.
7 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–6.
8 Ibid, Ch 26.
9 Rec 18–2.

policy reason for these discrepancies, agency-specific and organisation-specific requirements have been included within the 'Access and Correction' principle.[10]

Structure of the principle

29.13 The access and correction principles provided in the IPPs and the NPPs have significantly different structures. NPP 6 is an example of a 'hybrid principle'—that is, it contains some general, high-level provisions and some detailed, relatively prescriptive provisions.[11] NPP 6 first sets out the general rule that an organisation must provide an individual with access to personal information it holds about the individual. It then sets out an exhaustive list of exceptions to, qualifications of, and derogations from, this general rule, as well as a number of procedural provisions.

29.14 In comparison, IPPs 6 and 7 are limited to the general rules according to which an agency should provide an individual with access to, or permit correction of, personal information. The IPPs do not set out directly any exceptions to these rules. Rather, they defer to exceptions to access to, and correction of, personal information under any other 'law of the Commonwealth'.[12] In particular, this accommodates the exemptions from access and correction obligations set out in the FOI Act. The IPPs also do not include any procedural provisions for access to, and correction of, personal information. The Privacy Commissioner has advised, however, that agencies generally should process requests for access and correction under the *Privacy Act* in accordance with the administrative machinery set out in the FOI Act.[13]

29.15 This raises a question as to what is the appropriate structure for the 'Access and Correction' principle in the model UPPs.

29.16 In DP 72, the ALRC came to the preliminary view that the 'Access and Correction' principle in the UPPs generally should replicate the structure of NPP 6.[14] In particular, the ALRC noted that moving the detailed provisions of the 'Access and Correction' principle—for example, into another part of the *Privacy Act* or into regulation—would require the provisions to be redrafted so that they operate as conventional statutory provisions, as distinct from principles.[15]

---

10 See, for example, Rec 29–2.

11 For discussion of the overall structure of the privacy principles, see Ch 18.

12 See: *Privacy Act 1988* (Cth) s 14, IPPs 6, 7.2, 7.3(b).

13 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 13.

14 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [26.11]–[26.13].

15 The differences between principles-based regulation and rules-based regulation is discussed in Ch 4.

ALRC's view

29.17 NPP 6 provides an appropriate template for the 'Access and Correction' principle. Basing the 'Access and Correction' principle on NPP 6 is consistent with the ALRC's view that the NPPs should form the general template in drafting and structuring the UPPs.[16] In particular, the ALRC notes that the general structure of the NPPs largely has been effective. Furthermore, adopting a radically different structure from the NPPs would involve a greater compliance burden, particularly on organisations that would have to update their privacy protection regimes.

Application to third parties

29.18 Currently, the privacy principles only provide individuals with rights to obtain access to, and correction of, their personal information.[17] An agency is not required to provide an individual with access to a document if its disclosure would involve the unreasonable disclosure of personal information about any person, including a deceased person.[18] An organisation also is not required to provide access where providing such access would have an unreasonable impact on the privacy of other individuals.[19]

29.19 In its submission on DP 72, the Human Rights and Equal Opportunity Commission (HREOC) suggested that the proposed 'Access and Correction' principle should not 'unduly inhibit the ability of Indigenous people to access information needed to identify their natural families or communities'. HREOC submitted that agencies and organisations should be required to provide Indigenous persons with access to information that they need to identify their natural family or community—even if this involves an infringement of a third person's privacy.[20]

ALRC's view

29.20 In Chapter 7, the ALRC considers whether the protection of the *Privacy Act* should extend to groups and, in particular, Indigenous groups. The ALRC does not recommend that the *Privacy Act* be extended to provide direct protection to Indigenous or other racial, cultural or ethnic groups. It recommends, however, that information privacy rights and interests of Indigenous groups should be provided with additional protection—in particular, through the development of privacy protocols that respond to the particular privacy needs of such groups. If appropriate, these protocols could enable an individual to obtain access to personal information about another individual in certain circumstances.[21]

---

16 See Ch 18.
17 *Privacy Act 1988* (Cth) s 14, IPP 6; sch 3, NPP 6.
18 Ibid, IPP 6, *Freedom of Information Act 1982* (Cth) s 41.
19 *Privacy Act 1988* (Cth) sch 3, NPP 6.1(c). This exception has been retained in the model UPPs.
20 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.
21 Rec 7–1.

Recommendation 29–1 The model Unified Privacy Principles should contain a principle called 'Access and Correction' that, subject to Recommendation 29–2, applies consistently to agencies and organisations.

Access to personal information: general framework

29.21 This section considers how the access provisions of the 'Access and Correction' principle should be framed, including whether access should:

- be an obligation imposed on an agency or organisation or an entitlement of the individual;
- apply to information 'held' by an agency or organisation or information in its 'possession or control'; and
- include a provision for agencies to provide access to documents otherwise than as required by the *Privacy Act*.

29.22 Issues about access to personal information also arise in relation to exceptions to the requirement to provide access and alternative ways to provide individuals with access to personal information—namely, providing access through intermediaries. These issues are considered in following sections of this chapter.

An obligation or a right?

29.23 IPP 6 provides an individual with a right to obtain access to his or her personal information. In contrast, NPP 6 imposes an obligation on organisations to provide access to personal information.

29.24 In DP 72, the ALRC noted that it had not formed a strong view as to whether the provision dealing with access to personal information held by agencies should be expressed so as to grant an individual a right, or impose an obligation on an agency. Ultimately, it proposed that the access and correction provisions that apply to agencies should be expressed as an obligation on the agency, rather than an entitlement of an individual. That is, if an agency holds personal information about an individual the agency must, if requested to do so by the individual, provide the individual, with access to the information, subject to the relevant exceptions.[22]

22 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–8(a).

Submissions and consultations

29.25 Several stakeholders supported the proposal.[23] The Office of the Privacy Commissioner (OPC) supported the proposal but submitted that the nature of the proposed exceptions would have a significant bearing on whether the intent of the proposal was achieved.[24] Privacy NSW supported the proposal on the proviso that the existing provision in the FOI Act be referred to in the UPP itself, or that it be annexed to the *Privacy Act*.[25] The Australian Communications and Media Authority (ACMA) and the Australian Federal Police (AFP) argued for appropriate exemptions for law enforcement and regulatory functions.[26] No stakeholders opposed this proposal.

ALRC's view

29.26 The 'Access and Correction' principle in the model UPPs should provide that agencies and organisations must, if requested by the individual, provide the individual with access to his or her personal information (subject to the relevant exceptions). This approach was supported by a number of stakeholders. It also is consistent with the terminology that has been used in the other model UPPs.

'Possession or control' of personal information

29.27 IPPs 6 and 7 apply when personal information is in an agency's 'possession or control'. By contrast, NPP 6 applies when personal information is 'held' by an organisation. 'Possession and control' may be broader than the term 'held'. For example, an agency could administer a database—and therefore retain substantive control over it—but outsource physical possession of the database to another agency or organisation. In these circumstances, the agency would still have 'possession or control' for the purposes of IPPs 6 and 7. It is unclear, however, whether the agency 'holds' the information.

29.28 There is no clear guidance on when information is 'held' by an organisation for the purposes of NPP 6. Some direction may be provided, however, from judicial interpretation of documents 'in the possession of an agency' in the context of the FOI Act.[27] In *Beesley v Australian Federal Police*, Beaumont J held that documents in the possession of an agency included those documents in its 'constructive possession'—that is, where the agency had a right or power to deal with the document in question.[28] This precedent, however, was limited to records held in electronic form. Beaumont J expressly declined to overrule earlier cases which held that 'possession', when used in

---

23 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

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

25 Privacy NSW, *Submission PR 468*, 14 December 2007.

26 Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

27 *Freedom of Information Act 1982* (Cth) s 4(1).

28 *Beesley v Australian Federal Police* [2001] FCA 836.

the context of access to hard copies of documents under the FOI Act, meant documents in the physical possession of an agency.[29]

ALRC's view

29.29 Where personal information is under the control of one agency or organisation but in the possession of another, an individual should have the right under the *Privacy Act* to request access either from the administering agency or organisation or the agency or organisation that has actual possession of the information.

29.30 One way to achieve the above policy outcome is by interpreting documents 'held' by an agency or organisation as including those documents in its 'constructive possession'. This interpretation is consistent with case law about 'documents in the possession of an agency' for the purpose of the FOI Act. Retaining the term 'held' in the 'Access and Correction' principle also is consistent with the wording used in a number of other UPPs.[30]

29.31 If, however, Parliamentary Counsel does not consider the term 'held' to be broad enough to support access to personal information that is in the constructive possession of an agency or organisation, then the principle should be drafted in another way to include this concept. This could include, for example, applying expressly the 'Access and Correction' principle to personal information in the constructive possession of an agency or organisation.

29.32 The ALRC recommends, below, that the OPC should provide guidance on the 'Access and Correction' principle. This guidance should address the issue of when personal information is 'held' by agencies and organisations.[31]

Access other than under the *Privacy Act*

29.33 The FOI Act specifically permits an agency to provide access to documents otherwise than in accordance with the Act's requirements, provided that the agency can 'properly do so' or where such access is 'required by law'.[32] This provision may allow, for example, access to documents that are exempt under the FOI Act, such as internal working documents or documents relating to business affairs.[33] It also may permit access to documents without recourse to the (sometimes cumbersome) processes of the FOI Act.

---

29 See *Re Sullivan v Department of Industry, Science and Technology* (1996) 23 AAR 59 *and Information Commissioner for Western Australia v Ministry of Justice* (2001) WASC 3. The approach taken in these cases, however, was consistent with promoting, rather than impeding, access to information.

30 See, for example, the 'Openness' principle and the 'Data Security' principle.

31 Rec 29–9.

32 *Freedom of Information Act 1982* (Cth) s 14.

33 See Ibid pt IV.

Submissions and consultations

29.34 In DP 72, the ALRC expressed the preliminary view that an equivalent provision should be included in the *Privacy Act*.[34]

29.35 The OPC supported this proposal, but was concerned that the word 'properly' could have several meanings. It suggested that it be replaced with the word 'lawfully' or be clarified in some way.[35] The Department of Human Services submitted that the use of the term 'publishing' was inappropriate, given that personal information is rarely 'published', and suggested that the word 'communicates' may be preferable.[36]

ALRC's view

29.36 The ALRC's view on this issue has changed from that expressed in DP 72. The purpose of s 14 of the FOI Act is to ensure that an agency has the authority to publish or make government documents available, where appropriate, either on its own initiative or in response to a particular request, without recourse to the processes of the FOI Act. Such a provision is not required in the context of the *Privacy Act*, which is designed to provide a simple and user-friendly mechanism for individuals to access and correct their own personal information. Accordingly, the ALRC does not recommend that s 14 of the FOI Act be mirrored in the *Privacy Act*.

Access to personal information: exceptions

29.37 The IPPs and the NPPs place obligations on agencies and organisations to provide individuals with access to personal information that they hold about the individuals, unless a specific exception applies. There are a number of differences, however, between these exceptions. Questions therefore arise about:

- whether the 'Access and Correction' principle in the model UPPs should provide different exceptions to an individual's right of access, depending on whether the information is held by an agency or organisation; and

- what should be the content of such exceptions.

Different exceptions for agencies and organisations?

Background

29.38 As noted above, IPP 6 provides that an agency should provide an individual with access

---

34 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–8(c).

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

36 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

> 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.[37]

29.39 This provision generally limits the right to access personal information under the *Privacy Act* to the right to obtain access to information under Part IV of the FOI Act. For documents that are more than 30 years of age, the exemptions to access to documents under s 33 of the *Archives Act 1983* (Cth) may apply.

29.40 In comparison, the exceptions to an organisation's obligation to provide individuals with access to their personal information are set out in an exhaustive list in NPPs 6.1 and 6.2.

Submissions and consultations

29.41 In DP 72, the ALRC asked what exceptions should apply to an agency's obligation to provide an individual with access to personal information that it holds about him or her. In particular, the ALRC asked whether the exceptions should mirror the provisions in Part IV of the FOI Act, or whether another set of exceptions should apply.[38]

29.42 Some stakeholders were of the view that the provisions of Part IV of the FOI Act should be mirrored in the *Privacy Act*.[39] Others submitted that the exceptions that apply to organisations under the 'Access and Correction' principle also should apply to agencies.[40] ACMA submitted that it was essential that any exceptions recognise the public interest in law enforcement and regulatory agencies being able to fulfil their regulatory and enforcement functions.[41]

29.43 National Legal Aid submitted that an individual's interest in obtaining access to his or her personal information should be given a higher priority than access to other kinds of information. Accordingly, the barriers to access under the FOI Act should be reduced in the *Privacy Act*. It noted that the FOI Act contains provisions that attempt to reduce the barriers to access,[42] and submitted that these provisions could be extended and clarified in the *Privacy Act*.[43]

---

37 *Privacy Act 1988* (Cth) s 14, IPP 6.

38 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 12–1.

39 See, eg, Australian Government Department of Foreign Affairs and Trade, *Submission PR 563,* 24 January 2008; Australian Taxation Office, *Submission PR 515,* 21 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; Australian Government Department of Defence, *Submission PR 440,* 10 December 2007.

40 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.

41 Australian Communications and Media Authority, *Submission PR 522,* 21 December 2007.

42 See *Freedom of Information Act 1982* (Cth) ss 36(1)(b), 38(2).

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

ALRC's view

29.44 Exceptions to the 'Access and Correction' principle should be consistent with exemptions under the FOI Act. Similarly, the exceptions to the 'Access and Correction' principle should be consistent with exemptions under the *Archives Act*.[44] Agencies should not be subject to conflicting obligations under different legislative schemes in relation to the same information. Further, individuals should not be able to compel access to information under the *Privacy Act* that would otherwise be exempt under the FOI Act or the *Archives Act*.

29.45 Accordingly, the exemptions under the FOI Act should continue to apply to agencies when making decisions about access to personal information under the *Privacy Act*.[45] For information held in documents that are 30 years or more of age, the exemptions in the *Archives Act* should apply.[46]

29.46 The ALRC notes that some of the exemptions under the FOI Act are modified where an individual requests access to personal information about him or her, or disclosure of a document is in the public interest. For example, s 38(1) of the FOI Act, which provides that a document is exempt from disclosure if disclosure is prohibited by legislation, generally does not apply so far as the document in question contains personal information about the person requesting access to it.[47]

29.47 On 24 September 2007, following the release of DP 72, the then Attorney-General of Australia referred to the ALRC for inquiry and report matters relating to the extent to which the FOI Act and related laws continue to provide an effective framework for access to information in Australia. The issue of whether the FOI exemptions should be amended to deal with requests for access to personal information should be considered as part of that review.

What should be the content of the exceptions?

Background

29.48 Above, the ALRC recommends that, where an agency receives a request for access to, or correction of, personal information under the *Privacy Act*, the agency should continue to apply the relevant provisions set out in other federal laws—most notably, exempt documents under the FOI Act. Consequently, the exceptions to access provided in the 'Access and Correction' principle will apply only to organisations.

---

44 In this Report, an 'exception', as applied to the privacy principles, applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. Part IV of the FOI Act sets out a number of 'exempt documents', to which the access requirements of the FOI Act do not apply. Section 33 of the *Archives Act* sets out 'exempt records', to which the Act's access provisions do not apply.

45 Including exemptions under *Freedom of Information Act 1982* (Cth) ss 12, 13 and pt IV.

46 The exemptions in the *Archives Act* are similar to those in the FOI Act.

47 *Freedom of Information Act 1982* (Cth) s 38(2), (3).

29.49 Currently, NPP 6.1 includes a lengthy list of exceptions to an organisation's obligation to provide an individual with access to personal information, including (among others) where providing access would: have an unreasonable impact on the privacy of other individuals; relate to legal proceedings between the organisation and individual and would not be accessible through the discovery process; be unlawful; or prejudice investigation of a possible unlawful activity. Additionally, an organisation is not required to provide access to personal information it holds about an individual to the extent that:

> (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
>
> (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual …[48]

29.50 Furthermore, NPP 6.2 allows an organisation to give an individual an explanation of personal information, rather than direct access, 'where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process'.

Discussion Paper proposals

29.51 The 'Access and Correction' principle proposed in DP 72 primarily retained the exceptions to an individual's right to obtain access to personal information set out in NPP 6. The ALRC proposed one change, however, to the exception that allows an organisation to deny access where providing access would pose a serious threat to an individual's life or health. This was that the:

- two exceptions in NPP 6.1(a) and (b) should be consolidated into a single exception in the 'Access and Correction' principle in the proposed UPPs; and
- exception would apply where providing access to the personal information in question would be 'reasonably likely to pose a serious threat to the life or health of any individual'.[49]

29.52 This change reflected the ALRC's proposal that the 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use and disclose personal information if the use or disclosure was necessary to lessen or prevent a 'serious' (as opposed to a 'serious and imminent') threat.[50]

---

48 *Privacy Act 1988* (Cth) sch 3, NPP 6.1.
49 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 26–6.
50 Ibid, Proposal 22–3.

Submissions and consultations

Threat to life or health

29.53 The majority of stakeholders who commented on this issue supported the ALRC's proposal to remove the word 'imminent' from the exception to the 'Access and Correction' principle.[51] The Department of Human Services generally supported this proposal, but noted that determining whether access could pose a 'serious threat' often is not practicable in the context of the relationships of the Department and service delivery agencies with individuals.[52] The National Catholic Education Commission and Independent Schools Council of Australia supported the removal of the word 'imminent', but commented that they would prefer that the word 'significant' be used rather than the word 'serious'.[53] One stakeholder advised that it failed to see 'why a right of access should be given priority over *any* threat to the life or health of an individual'.[54]

29.54 The OPC disagreed with the proposal. It submitted that—other than in the context of health information—the 'Access and Correction' principle should retain the 'serious and imminent' test for threats to the life or health of an individual. The OPC was concerned that removing the existing requirement for the threat to be imminent, and allowing an organisation to deny access to an individual on the grounds that 'such access would be reasonably likely to pose a serious threat to the life or health of any individual', would unjustifiably lower the current privacy protections offered under NPP 6. The OPC acknowledged, however, that the removal of the 'imminent' test might be justified in the context of the disclosure of health information, particularly mental health information or other information that may have a 'highly emotional element'.[55]

29.55 Some other stakeholders supported retaining the words 'serious and imminent threat' in the 'Access and Correction' principle, as well as the principles dealing with the collection of sensitive information and the use and disclosure of personal information.[56] On a related issue, one stakeholder submitted that

> it is not clear what the intention of the ALRC is in modifying the grounds on which access by an individual to their personal information should be able to be refused

---

51 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

52 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

53 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

54 Confidential, *Submission PR 536*, 21 December 2007.

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

56 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Optus, *Submission PR 532*, 21 December 2007.

from when providing access 'would pose a serious threat' to the life or health of any individual to where this 'would be reasonably likely to pose a serious threat'.[57]

Other exceptions to access rights

29.56 Some stakeholders submitted that other exceptions in the proposed 'Access and Correction' principle were not sufficiently stringent. Concerns were expressed about the exceptions permitting an organisation to deny an individual access to his or her personal information if: denying access is required or authorised by or under law;[58] providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; [59] and providing access would be likely to prejudice activities 'by or on behalf of an enforcement body'.[60] Liberty Victoria submitted that, other than in the context of a criminal investigation, individuals always should be able to access and correct personal information held by agencies or organisations.[61]

29.57 Avant Mutual Group Ltd noted that the exception for existing or anticipated legal proceedings should be consistent with the common law and the provisions of the *Evidence Act 1995* (Cth) relating to client legal privilege.[62]

29.58 Privacy advocates also raised concerns about the exception set out in the proposed UPPs, which would permit an organisation to provide an individual with an explanation for a commercially sensitive decision, rather than direct access to the information.[63] The Cyberspace Law and Policy Centre, for example, was concerned that this exception could be used to deny direct access to personal information in situations where such access would be appropriate. The Centre also commented that the note following UPP 9.2[64] was tautologous. The Centre submitted that this note should be replaced by one advising that 'the mere fact that some explanation may be necessary in order to understand information such as a score or algorithm result should

57 Confidential, *Submission PR 570*, 13 February 2008.
58 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.
59 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
60 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
61 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.
62 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.
63 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.
64 This note stated, 'an organisation breaches UPP 9.1 if it relies on UPP 9.2 to give an individual an explanation for a commercially sensitive decision in circumstances where UPP 9.2 does not apply'.

not be taken as grounds for withholding information'.[65] Privacy NSW submitted that this exception should be incorporated into UPP 9.1.[66]

ALRC's view

Threat to life or health

29.59 An individual should not be entitled to obtain access to personal information that an organisation holds about him or her if providing access would pose a serious threat to the life or health of any individual (including the individual seeking access). There should not be a further requirement that this threat is 'imminent'. This is consistent with the change that the ALRC is recommending to the exception under the 'Use and Disclosure' principle.[67]

29.60 In Chapter 25, the ALRC discusses the meaning of 'serious threat' in the context of the recommended exception to the 'Use and Disclosure' principle. It notes that the ALRC's recommendation that the 'imminent' threat requirement be removed means that an assessment of *when* a threat will take place is no longer required. An assessment of *whether* a threat is likely to eventuate, however, still will be necessary. This discussion applies equally in the context of denying an individual access to personal information.

29.61 The exception to an organisation's obligations to provide an individual with access to his or her personal information where it would pose a serious threat to life or health should apply where such a threat is 'reasonably likely' to occur. In most situations, an organisation will not be able to conclude definitively that providing an individual with access to his or her personal information 'will' pose a serious threat to an individual's life or health. This uncertainty has been dealt with in the language used in the other contexts where it arises. For example, in the 'Use and Disclosure' principle, the information may be used or disclosed where an agency or organisation 'reasonably believes' the use or disclosure is necessary to lessen or prevent such a threat. Similarly, under the FOI Act, an agency can deny a request for access where disclosure 'would, or could reasonably be expected to endanger the life or physical safety of any person'.[68]

29.62 This recommendation may increase the likelihood that an individual will be denied access to his or her personal information. The ALRC is making a number of recommendations, however, that will lessen the detriment resulting from a refusal of access. In particular, the ALRC recommends that, where an agency or organisation considers that it is not required to provide an individual with access to personal information, it must take reasonable steps to provide the individual with as much of the

---

65 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
66 Privacy NSW, *Submission PR 468*, 14 December 2007.
67 Rec 25–3.
68 *Freedom of Information Act 1982* (Cth) s 37(1).

information as possible. This could include providing information through a mutually agreed intermediary.[69] A more stringent intermediary provision is recommended where an organisation denies an individual access to his or her health information because providing access would be reasonably likely to pose a serious threat to any individual.[70] These provisions offset sufficiently any lessening of individuals' rights to access their own personal information that may result from broadening this exception.

Other exceptions to access rights

29.63 With the exception of the change recommended above, the 'Access and Correction' principle should include the existing exceptions in NPP 6. These exceptions—for example, where denying access is required or authorised by or under law, or where providing access could prejudice law enforcement activities—balance appropriately the public interest in safeguarding the handling of personal information with competing public interests.

29.64 The ALRC agrees with the Cyberspace Law and Policy Centre, however, that the statutory note presently set out in NPP 6 (that 'an organisation breaches NPP 6.1 if it relies on NPP 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where UPP 9.2 does not apply') is tautologous and should be removed. A statutory note should be included in the 'Access and Correction' principle stating that the mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information.

Recommendation 29–2 The 'Access and Correction' principle should provide that:

(a) if an agency holds personal information about an individual, the individual concerned is entitled to have access to that personal information, except to the extent that the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; and

(b) subject to Recommendation 29–3, if an organisation holds personal information about an individual, the individual concerned shall be entitled to have access to that personal information, except to the extent that one of the exceptions to the right of access presently set out in National Privacy Principle 6.1 or 6.2 applies.

69 Rec 29–4.
70 Rec 63–6.

Recommendation 29–3 The 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual, it is not required to provide access to the information to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of any individual.

Access to personal information: intermediaries

Background

29.65 NPP 6.3 currently requires an organisation that has lawfully denied an individual access to his or her personal information to consider providing access to the information to a mutually agreed third party intermediary. The object behind this provision was explained in the Explanatory Memorandum and other material accompanying its introduction:

> [NPP 6.3] is not intended to provide a mechanism to reduce access if access would otherwise be required. There will be some cases—investigations of fraud or theft for example—where no form of access is appropriate. In other cases, it should be considered as an alternative to complete denial of access. For example, in the health context, an intermediary could usefully explain the contents of the health record to the individual as an alternative to denying access to the health information altogether.[71]

29.66 In other words, NPP 6.3 requires an organisation to consider whether a compromise can be reached that would allow an individual some form of indirect access to his or her personal information in circumstances where direct access is not appropriate. The IPPs do not contain an equivalent provision. The FOI Act, however, provides that where an agency denies a request for access to a document containing personal information, provided by a 'qualified person',[72] on the basis that disclosure of the information might be detrimental to the applicant's physical or mental health or well-being, the agency may provide access to the document through another qualified person nominated by the applicant.[73]

29.67 The OPC, in its review of the private sector provisions of the *Privacy Act* (the OPC Review), noted concerns that the obligation in NPP 6.3 for an organisation to

---

71 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [376]. See also Office of the Federal Privacy Commissioner, *Access and the Use of Intermediaries*, Information Sheet 5 (2001).

72 'Qualified person' is defined in the Act to mean 'a person who carries on, and is entitled to carry on, an occupation that involves the provision of care for the physical or mental health of people or for their well being'. It includes a non-exhaustive list of such people, including a: medical practitioner; psychiatrist; psychologist; marriage guidance counselor; and social worker: *Freedom of Information Act 1982* (Cth) s 41(8).

73 Ibid s 41.

'consider' the use of intermediaries, where the organisation is not required to provide access, is inadequate.[74]

Discussion Paper proposals

29.68 In DP 72, the ALRC proposed that the 'Access and Correction' principle should provide that an organisation must take 'reasonable steps' to reach an appropriate compromise, involving the use of a mutually agreed intermediary in certain circumstances. The ALRC proposed that the OPC should provide guidance about what would be 'reasonable steps' in this context.[75] 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.[76]

Submissions and consultations

Organisations

29.69 A large number of stakeholders supported the proposition that an organisation that is not required to provide an individual with access to his or her personal information should take reasonable steps to provide access to the information through a mutually agreed intermediary.[77] Optus, for example, submitted that

> the proposed 'Access and Correction' principle should make it clearer that an organisation should give more than cursory consideration to whether a mutually agreed intermediary should be used in instances where a request to access information is legitimately refused.[78]

29.70 Some stakeholders suggested ways to improve the operation of the proposed provision. These included removing the qualification, 'provided that the compromise would allow sufficient access to meet the needs of both parties', which was considered unnecessarily restrictive.[79] The Cyberspace Law and Policy Centre and the Australian Privacy Foundation also suggested that the Privacy Commissioner should be

---

74 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 114, 116.

75 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 26–2.

76 Ibid, Proposal 12–8(c).

77 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

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

79 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

empowered to act as an intermediary, if requested by the parties, or in the event that the parties are unable to agree on an alternative intermediary.[80]

29.71 The Australian Bankers' Association Inc (ABA) and Suncorp-Metway Ltd supported the ALRC's proposal in principle, but noted that it should not be mandatory for the organisation to engage a mutually agreed intermediary where the organisation itself is capable of taking other reasonable steps to achieve a compromise regarding access to the information. Other reasonable steps could include, for example, the use of an external dispute resolution scheme.[81] Other stakeholders submitted that the existing provisions were adequate, considering the limited circumstances in which access can be denied.[82] The Attorney-General's Department (AGD) suggested an exception to the provision where taking reasonable steps to reach a compromise could prejudice the detection or investigation of unlawful activity.[83]

29.72 A number of stakeholders also supported the proposal that the OPC should provide guidance about the meaning of 'reasonable steps' in this context.[84] Privacy advocates expressed concern that organisations could use the existence of grounds for withholding some information as an excuse for denying access in its entirety. Accordingly, they suggested that the OPC guidance should address the need for organisations to withhold personal information to the minimum extent necessary.[85]

Agencies

29.73 The majority of stakeholders that commented on this issue supported requiring an agency to take reasonable steps to reach a compromise by providing access through a mutually agreed intermediary.[86] Privacy NSW, for example, noted that unless there is an equivalent provision for agencies, there will be differing levels of access rights for individuals, depending on whether the personal information is held by an agency or organisation.[87] The AFP and ACMA highlighted the need for exemptions to allow law

---

80 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

81 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

82 Confidential, *Submission PR 536*, 21 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

83 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

84 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007.

85 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

86 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

87 Privacy NSW, *Submission PR 468*, 14 December 2007.

enforcement and regulatory agencies properly to perform their functions.[88] ACMA also was concerned about the resource implications of the proposal.[89]

ALRC's view

29.74 A provision requiring an agency or organisation to take reasonable steps to provide an individual with as much personal information as possible, in circumstances where access to the information legitimately can be refused, is important. Such a provision allows for a more flexible, nuanced approach to requests for access where direct access is not appropriate. One such reasonable step is the use of an intermediary. The benefits of an intermediary provision apply equally whether information is held by an agency or organisation.

'Reasonable steps' to provide access

29.75 The present requirement in NPP 6.3—that an organisation must 'consider' the use of a mutually agreed intermediary—potentially is open to abuse. Technically, the requirement would be fulfilled where an organisation briefly contemplates, and then immediately rejects, such a course of action.

29.76 The proposal that an agency or organisation should take 'reasonable steps' to reach an appropriate compromise regarding access to personal information, where such access legitimately can be refused, received considerable support from stakeholders. Law enforcement and regulatory agencies were concerned, however, that a requirement to take 'reasonable steps' may not clarify sufficiently that, in some circumstances, it would not be appropriate for an agency or organisation to take any steps to provide access.

29.77 The intermediary requirement should provide that agencies and organisations must take 'such steps, if any, as are reasonable'.[90] This will ensure that the requirement is stringent enough that agencies and organisations must give more than superficial consideration to the use of an intermediary. The revised wording of the requirement remains sufficiently flexible to accommodate situations where the circumstances justify the agency or organisation taking no steps to provide access. This may be the case, for example, where an agency is investigating unlawful activity. The OPC, in its guidance on the 'Access and Correction' principle, should address what would be considered 'reasonable steps' in this context.[91]

---

88 Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

89 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

90 This wording is consistent with that in the 'Notification' principle.

91 See Rec 29–9.

Reaching an 'appropriate compromise'

29.78 The intermediary requirement proposed in DP 72 required organisations to 'reach an appropriate compromise' with individuals seeking access to their personal information. This wording potentially is ambiguous. This requirement can be stated more clearly as being to 'provide the individual with as much of the information as is possible'.

29.79 In addition, the ALRC agrees with stakeholders that the proposed wording—'provided that the compromise would allow sufficient access to meet the needs of both parties'—may restrict the operation of the principle unnecessarily. For example, there will be circumstances where a compromise may not be sufficient to meet the needs of both parties, but remains preferable to refusing access. These words, therefore, have not been included in the recommended 'Access and Correction' principle.

A 'mutually agreed' intermediary

29.80 As framed, the 'Access and Correction' principle in the model UPPs is limited to situations where the parties can agree on an intermediary. It does not contain a 'circuit breaker' to deal with situations where the parties fail to reach such an agreement. In Chapter 63, the ALRC recommends that, where an organisation denies an individual access to his or her health information on the grounds that it is reasonably likely to pose a serious threat to any individual, the individual should have the right to nominate a health service provider and request that the organisation provide the nominated health service provider with access to the information.[92] Considering the large number of access complaints that relate to health information,[93] this procedure could apply to many situations where mutual agreement on an intermediary cannot be reached.

29.81 It is possible that an officer of the OPC may, in some situations, agree to act as an intermediary. The decision to take on any such role will be dependent on the OPC being sufficiently resourced, and the relevant officer being appropriately qualified.

Access other than through an intermediary

29.82 Providing access through the use of a mutually agreed intermediary is not the only way that an agency or organisation may provide limited access to personal information. Other ways include, for example, giving a verbal summary of the personal information, excluding the information covered by the exception.[94] The ALRC

---

92 See Rec 63–6.

93 Of the 330 NPP complaints against health care providers received by the OPC between 21 December 2001 and 31 January 2005, 163 concerned a refusal of access to health records. Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 112.

94 Office of the Federal Privacy Commissioner, *Access and the Use of Intermediaries*, Information Sheet 5 (2001).

recommends, therefore, that the reasonable steps taken by an agency or organisation to reach an appropriate compromise should *include* the use of an intermediary.

Recommendation 29–4 The 'Access and Correction' 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.

Correction of personal information

Background

29.83 Where an agency or organisation holds incorrect personal information about an individual, in most circumstances the individual has the right to have this information corrected.

29.84 Under IPP 7.1, an agency that has possession or control of a record containing personal information must take reasonable steps by way of making appropriate corrections, deletions and additions to ensure that the information is accurate and is relevant, up-to-date, complete and not misleading. When assessing whether personal information satisfies these criteria, an agency must have regard to the purpose for which the information was collected, or is to be used, and any purpose that is directly related to that purpose.[95]

29.85 IPP 7.2 states that the obligation imposed on agencies to correct personal information 'is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents'. Such a limitation is found in Part V of the FOI Act, which sets out a number of procedural steps that an individual seeking the correction of personal information must take before the information can be corrected.

29.86 In comparison, NPP 6.5 provides that an organisation must take reasonable steps to correct personal information that it holds where an individual establishes that the information is not 'accurate, complete and up-to-date'.[96]

29.87 These correction provisions raise the following issues:

95 *Privacy Act 1988* (Cth) s 14, IPP 7.1(b).
96 Ibid sch 3, NPP 6.5–6.6.

- the criteria by which personal information is assessed as being 'correct', including how these criteria should be assessed;

- any burden of proof an individual must meet to establish that personal information that an agency or organisation holds about him or her is not 'correct';

- the manner of correcting personal information that has been found not to meet the correction criteria; and

- the relationship between the correction requirements under the *Privacy Act* and other federal laws.

29.88 Another issue that arises when an agency or organisation has corrected personal information under the 'Access and Correction' principle is the circumstances (if any) in which it is appropriate for that agency or organisation to notify third parties of the correction.

What is 'correct' personal information?

Background

29.89 Whether information is 'correct' for the purposes of the *Privacy Act* is not necessarily self-evident. Rather, this will depend upon the criteria by which the correctness of personal information is assessed. These criteria currently differ for agencies and organisations.

29.90 As noted above, NPP 6.5 enables an individual to request an organisation to correct personal information that is not 'accurate, complete and up-to-date'.[97] In addition to information that is not accurate, complete and up-to-date, IPP 7.1 also requires agencies to correct personal information that is irrelevant or misleading.[98]

29.91 In some situations, the correctness of personal information will depend on the context in which the information is assessed. For example, a medical record might include a diagnosis that is later demonstrated to be false. Clearly, where the record is being considered in the context of patient treatment, the information it contains would not be 'accurate' or 'up-to-date'. Where the record is being considered in another context—for example, as a historical record or for pending litigation—the information may be 'correct'.

29.92 The IPPs provide some assistance to agencies seeking to determine whether personal information is complete, up-to-date, relevant and not misleading. IPP 7.1(b) provides that whether personal information is complete, up-to-date, relevant and not

---

97 Ibid sch 3, NPP 6.5–6.6.
98 Ibid s 14, IPP 7.1.

misleading must be determined 'having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose'. The NPPs do not include any equivalent criteria against which to assess whether personal information is 'correct'.

29.93 There is a close relationship between the correction criteria provided in the 'Access and Correction' principle, and obligations on agencies and organisations to maintain the quality of personal information that they hold. NPP 3 (Data Quality) currently requires an organisation to take reasonable steps to ensure that personal information it collects, uses or discloses is 'accurate, complete and up-to-date'.[99]

29.94 At present, agencies are not subject to a 'stand-alone' data quality principle. Aspects of data quality, however, are included in other IPPs. IPP 3 provides, for example, that, where an agency collects personal information, it must take steps to ensure that information it collects is relevant to the purpose of collection and is up-to-date and complete.[100] IPP 8 also imposes data quality requirements on agencies when they use personal information.

Discussion Paper proposals

29.95 In DP 72, the ALRC proposed two changes to the existing principles relating to the right to correct personal information held by an organisation, aimed at achieving consistency between the 'Data Quality' principle and the 'Access and Correction' principle in the model UPPs:

- an individual should have the right to correct personal information that an organisation holds about him or her if it is not 'relevant'; and

- an organisation should be required to consider 'a purpose of collection permitted by the UPPs', when determining whether the personal information is correct.[101]

29.96 Similarly, in the context of agencies, the ALRC proposed that an agency should consider whether personal information is correct with reference to 'a purpose of collection permitted by the UPPs'.[102]

Submissions and consultations

29.97 Most stakeholders that commented on this issue supported the two proposed changes to the correction criteria for organisations.[103] Privacy advocates, however,

---

99 Ibid sch 3, NPP 3.
100 Ibid s 14, IPP 3. This requirement only applies to 'solicited' personal information.
101 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 26–5.
102 Ibid, Proposal 12–9(a).
103 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money

were concerned that the qualification 'with reference to a purpose of collection permitted by the UPPs' would allow an organisation to decline to correct personal information on the grounds that, while the information may be incorrect in relation to the purpose for which it was collected, it is not 'incorrect' in relation to *another* purpose for which the information is being used.[104]

29.98 Some stakeholders also supported the proposed change to the correction criteria for agencies.[105] Privacy NSW supported the proposal provided the existing provisions in the FOI Act are referred to in the 'Access and Correction' principle itself, or that it is annexed to the *Privacy Act*.[106] ACMA was concerned that the proposals may compromise the law enforcement and regulatory functions of agencies. It also had concerns about potential resource implications.[107]

ALRC's view

29.99 Individuals should be provided with the right to correct personal information held by agencies and organisations where the information is misleading or not accurate, relevant, up-to-date or complete. These elements are the same as those currently in the correction principle in the IPPs. Two of the elements, however, are additional to those set out in the correction principle in the NPPs—that is, that the information should be 'relevant' and 'not misleading'.

Criterion of 'relevance'

29.100 In most situations, an agency or organisation that holds personal information that is not relevant should destroy it, or render it non-identifiable, in accordance with the 'Data Security' principle.[108] In some situations, however, whether personal information is 'irrelevant' may be contextual. For example, an agency or organisation may hold personal information that is relevant for one of its functions or activities but not another. In these situations, the individual about whom the information relates should have the right to have the information deleted from (or otherwise corrected in) those records where it is irrelevant. As noted above, the proposal that individuals should have the right to correct personal information held by organisations if it is not 'relevant' was supported by a broad range of stakeholders.

Criterion of 'not misleading'

29.101 The recommended right of an individual to correct 'misleading' personal information that an organisation holds about him or her is new. This component,

---

Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

104 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

105 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

106 Privacy NSW, *Submission PR 468*, 14 December 2007.

107 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

108 See Ch 28.

however, is currently applicable to credit reporting agencies and credit providers in respect of personal information in credit information files and credit reports.[109] The ALRC does not anticipate that including a right for individuals to correct misleading personal information would impose a significant new compliance burden on organisations. In a large number of situations, misleading information will not be 'accurate', 'complete' or 'up-to-date' and, therefore, is already subject to the correction requirement in the NPPs.

29.102 Where information is 'misleading', but is otherwise accurate, complete, up-to-date and relevant, this will result in a difference between the correction requirements in the 'Access and Correction' principle and the requirements of the 'Data Quality' principle. The ALRC considers this discrepancy to be appropriate, however, in light of the different contexts in which these principles operate.

29.103 It is difficult for agencies and organisations to determine whether personal information is 'not misleading'. They may not be aware, for example, of surrounding circumstances that make the information 'misleading' in the absence of specific advice from the individual. When an individual exercises his or her right of correction, however, it is appropriate for an agency or organisation to assess, in a specific context, whether personal information is or is not misleading. This distinction presently is reflected in the IPPs, which provide individuals with a right to correct misleading information, but do not impose an independent requirement on agencies under IPP 8 to ensure that personal information is 'not misleading' before they use it.

Reference for assessing correction criteria

29.104 Data quality, as provided for in the 'Data Quality' principle, should be assessed with reference to the purpose for which information is being collected, used or disclosed.[110] In the context of the 'Access and Correction' principle, the correctness of information should be ascertained by reference to the purpose for which the information is being held.

29.105 In accordance with the ALRC's recommended 'Data Security' principle, an agency or organisation only should hold personal information where it is needed for a purpose for which the information can be used or disclosed under the UPPs, or where retention otherwise is required or authorised by or under law.[111] The purpose justifying retention of the information under the 'Data Security' principle also should be taken into account when assessing the correctness of the information under the 'Access and Correction' principle.

---

109 *Privacy Act 1988* (Cth) s 18J.
110 The 'Data Quality' principle is discussed in Ch 27.
111 The 'Data Security' principle is discussed in Ch 28.

Establishing that personal information is not correct

29.106 NPP 6.5 provides that, before an organisation is required to correct personal information, the individual to whom it relates must establish that the information is not accurate, complete and up-to-date. In the OPC Review, the OPC expressed concern that this requirement may be unclear and could impose 'an unduly high standard' on the individual seeking to correct his or her personal information.[112] In comparison, IPP 7 places agencies under a positive obligation to take steps to ensure that personal information that they hold is correct. This operates independently of the individual establishing that the information is not correct.

Submissions and consultations

29.107 In DP 72, the ALRC did not propose a change to the requirement in NPP 6.5 that an individual should establish that personal information is not correct. Several stakeholders, however, expressed concerns that to require individuals to establish that their personal information is not accurate, complete and up-to-date is excessively onerous.[113] The OPC submitted that there is

> a perceived lack of certainty regarding how an individual should satisfy the requirement of 'seek to establish that information is not accurate, complete or up-to-date'. Equally, it is unclear to what degree of certainty an individual must 'seek to establish' this, including to the Privacy Commissioner's satisfaction in the event of a complaint.[114]

29.108 Stakeholders suggested reframing the 'Access and Correction' principle to require an organisation to correct personal information where an individual: provides the organisation with 'reasonable grounds' to believe that the information that is held about them is in need of correction;[115] or establishes the need for correction on the balance of probabilities.[116] Liberty Victoria submitted that:

> If an individual contests that information is correct, they must have the opportunity to provide evidence or require the agency to check their information and have it corrected.[117]

ALRC's view

29.109 By requiring an agency or organisation to correct personal information if an individual 'is able to establish' that the information is not correct, without providing

---

112 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 118.

113 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

115 Ibid.

116 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

117 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.

for the requisite burden of proof, NPP 6.5 results in uncertainty in the event of a complaint.

29.110 The 'Access and Correction' principle should require agencies and organisations to ensure that the personal information they hold is, in accordance with the requisite correction criteria, correct. The words 'and the individual is able to establish that the information is not', therefore, should not be replicated in the principle. This approach is consistent with the approach currently taken in the IPPs and, accordingly, will not affect the existing practices of agencies. In addition, the ALRC does not anticipate that the change will affect significantly the practical operation of the correction requirements for organisations. Where an individual seeks to correct personal information that an organisation holds about him or her, the individual and organisation still must take steps to demonstrate that the information is, or is not, correct. This change has the principal advantage, however, that in the event of a complaint the relevant issue is the correctness of the personal information that is held by the agency or organisation.

Manner of correcting personal information

29.111 Where personal information held by an agency or organisation is 'incorrect', the agency or organisation must decide how to correct it. For example, should incorrect information be deleted, or should it clearly be marked as being superseded, while still remaining as a historical record?

29.112 The existing requirements in the NPPs are that an organisation must 'correct' personal information—they do not provide further guidance on what form this correction might take. The IPPs provide that an agency should make 'appropriate corrections, deletions and additions as are, in the circumstances, reasonable'. More detail still is set out in the FOI Act, which provides that, where an agency amends a record, it must, to the extent that it is practicable to do so, 'ensure that the record of information is amended in a way that does not obliterate the text of the record as it existed prior to the amendment'.[118]

29.113 Some guidance about how personal information should be corrected is available in the context of the FOI Act. In *Re Cox and Department of Defence*, the Administrative Appeals Tribunal advised that, when an agency considers the most appropriate manner in which to amend information under the FOI Act, it should consider whether the record: purports to be an objective recording of factual material; serves a continuing purpose; or may, if retained in an unamended form, serve a historic purpose.[119]

---

118 *Freedom of Information Act 1982* (Cth) s 50(3).

119 *Re Cox and Department of Defence* (1990) 20 ALD 499.

Submissions and consultations

29.114 Although no proposal specifically addressed this issue, some stakeholders, in response to DP 72, noted the potential tension between the obligation to correct personal information and archiving responsibilities. Privacy advocates suggested that the Privacy Commissioner should issue guidance noting that correction of personal information can take the form of amendment, deletion or addition, as appropriate in the circumstances. They suggested that this guidance should state that, where there is a legal requirement of keeping historical records of transactions, operational records can be corrected and the original incorrect information retained as an archive.[120]

29.115 The National Archives of Australia expressed concerns about any changes to the FOI Act that make it easier for personal information to be deleted without regard for other record-keeping requirements. The National Archives suggested that it is more appropriate to amend or correct a record without obliterating the evidence on which a decision had been made, than to delete the information.[121]

ALRC's view

29.116 Personal information may be corrected in a number of ways, including by directly amending the material, deleting the incorrect material, or adding to the material. The appropriate method of correction will depend on the circumstances of the case. The ALRC recommends, below, that the OPC should develop and publish guidance on the 'Access and Correction' principle.[122] This guidance should address the manner in which personal information can be corrected, and discuss potential conflicts between the requirements of the 'Access and Correction' principle and other record-keeping obligations, including those under the *Archives Act*.

Correction obligations under the *Privacy Act* and other federal laws

29.117 As noted above, the obligation imposed on agencies to correct personal information 'is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents'.[123] The relationship between correction requirements under the *Privacy Act* and the FOI Act is discussed in Chapter 15. For the reasons set out in that chapter, the ALRC is of the view that individuals should continue to be able to access and correct personal information under the *Privacy Act* and the FOI Act.

29.118 The ALRC has received Terms of Reference to review the operation of the FOI Act and related laws. The ALRC's FOI Inquiry could consider recommending that the FOI Act should be amended so that it no longer regulates access to, and correction of, personal information.

---

120 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

121 National Archives of Australia, *Submission PR 414*, 7 December 2007.

122 Rec 29–9.

123 *Privacy Act 1988* (Cth) s 14, IPP 7.2.

Incorrect information: notification of third parties

29.119 Where an agency or organisation has corrected personal information in accordance with the 'Access and Correction' principle, there is a question whether it should be required to notify third parties of this correction and, if so, in what circumstances this obligation should arise.

29.120 The IPPs and the NPPs currently do not include a requirement for an agency or organisation to notify third parties of personal information that it has corrected. Such an obligation is found, however, in a number of international instruments and laws. For example, the EU Directive states that member states must guarantee that every data subject has the right to require the data controller to notify

> third parties to whom the data have been disclosed of any rectification, erasure or blocking out [that has been carried out where the data are incomplete or inaccurate] unless this proves impossible or involves a disproportionate effort.[124]

29.121 Canadian privacy law requires organisations, where appropriate, to transmit corrected personal information to third parties, or to notify those parties of an unresolved challenge concerning the accuracy of the personal information.[125] It also states that, in certain circumstances, a government entity that has disclosed personal information to third parties must notify the third party of any correction made to that information or of any notation where the correction is not made.[126] In Germany, public and private bodies must, 'if necessary to protect legitimate interests of the data subject', notify third parties to which data have been transmitted of 'the correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage'.[127]

29.122 New South Wales privacy law also requires New South Wales agencies to notify third parties of incorrect information. Section 15(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) provides that, if personal information is amended by an agency, the individual to whom the information relates is entitled, if reasonably practicable, to have recipients of that information notified of the amendments.[128]

---

124 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 12(c). See also the United States Federal Trade Commission, which in identifying core principles of data protection, has stated that 'to be meaningful, access must encompass … the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients': United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998), 9.

125 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principles 4.9.5, 4.9.6.

126 *Privacy Act* RS 1985, c P-21 (Canada) s 12(2).

127 *Federal Data Protection Act 1990* (Germany) ss 20(8), 35(6).

128 *Privacy and Personal Information Protection Act 1998* (NSW) s 15(3).

29.123 The OPC Review recommended that

> the Australian Government should consider amending NPP 6 to provide that when an individual's personal information is corrected in response to a request from the individual, the organisation should be obliged to notify third parties, where practicable, that they have received the inaccurate information.[129]

Issues Paper question

29.124 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* should be amended to impose an obligation on agencies and organisations to notify third parties that they have received inaccurate information and to pass on any corrected information.[130] A number of stakeholders supported this requirement.[131] Some limitations also were suggested, including: that the obligation should be triggered only at the request of the individual concerned;[132] that any requirement to notify third parties should apply only where the inaccuracy is 'material';[133] and that the requirement should apply only 'where reasonable and/or practicable'.[134]

Discussion Paper proposal

29.125 In DP 72, the ALRC proposed that an agency or organisation should be required to take reasonable steps, where practicable, to notify any third party to whom it had disclosed personal information, of any correction to that information, providing that it is requested to do so by the individual to whom the information relates.[135]

Submissions and consultations

29.126 A number of stakeholders supported the ALRC's proposals for notification of third parties by agencies[136] and organisations.[137] Some stakeholders suggested that the

---

129 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 28.

130 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–25.

131 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; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 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; K Pospisek, *Submission PR 104,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

132 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.

133 AAMI, *Submission PR 147,* 29 January 2007.

134 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

135 Australian Law Reform Commission, *Review of Australian Privacy Law,* DP 72 (2007), Proposals 12–9(b), 26–4.

136 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; Australia Post, *Submission PR 445,* 10 December 2007.

circumstances in which the notification requirement applies should be broader than where the individual requests notification, to cover, for example, situations where the individual may not have the capacity to make such a request[138] or where the individual may not be aware of the error.[139]

29.127 Other stakeholders, however, were concerned about the resource implications of the proposals for agencies[140] and organisations.[141] In particular, stakeholders expressed concerns about the need for agencies and organisations to identify and track all third party disclosures, including one-off data transfers.[142]

29.128 A number of stakeholders also commented that the proposed notification requirements placed an inappropriate burden on agencies and organisations.[143] GE Money Australia, for example, noted that the proposal did not take into account the reasons why the information needed to be corrected.

> The proposal appears to have implicit in it that there is fault on the part of the organisation by reason of it having and having disclosed information that may not be correct or up to date. Incorrect or unclear information may have been provided to it in the first instance. It may be practicable for an organisation to notify other entities but this does not mean that in all circumstances it should be the organisation that should do so.[144]

29.129 ANZ expressed the view that the current privacy principles dealing with the correction of personal information were adequate. It suggested, however, that, if the proposal to notify third parties were to be adopted, it should apply only 'where

---

137 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 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; Smartnet, *Submission PR 457*, 11 December 2007.

138 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

139 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

140 Social Security Appeals Tribunal, *Submission PR 478*, 17 December 2007. See also Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

141 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; BPay, *Submission PR 566*, 31 January 2008; Acxiom Australia, *Submission PR 551*, 1 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; ANZ, *Submission PR 467*, 13 December 2007.

142 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; BPay, *Submission PR 566*, 31 January 2008; Confidential, *Submission PR 536*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

143 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007.

144 GE Money Australia, *Submission PR 537*, 21 December 2007.

inaccuracies are considered by a reasonable person to be material and [notification] would be practicable in the circumstances'.[145] Acxiom Australia also was of the view that the proposed obligation should apply only where the inaccuracy is 'material'.[146] The Law Council of Australia noted that it would be necessary to clarify the rights and obligations of third parties that have received incorrect personal information.[147]

ALRC's view

29.130 Where an agency or organisation has corrected personal information, it should be required to notify any other entities to which it has disclosed the information of the correction, if requested to do so by the individual. In particular, this will reduce the risk that any entities to which the incorrect personal information has been disclosed will use or disclose the information inappropriately at a later time.

29.131 The potential costs of compliance were the major cause of concern. In particular, stakeholders were concerned that the notification provision would require agencies and organisations to log all disclosures of personal information.[148] The ALRC considers that the requirement to take 'reasonable steps' provides sufficient flexibility to cover all situations adequately. Concerns can be addressed sufficiently by clarifying that reasonable steps may, in some situations, equal no steps.

29.132 Guidance on the 'Access and Correction' principle[149] should address the factors that an agency or organisation should consider when it assesses whether it would be reasonable and practicable to notify third parties that it has disclosed incorrect information. These could include:

- whether the agency or organisation has an ongoing relationship with the entity to which it has disclosed the information;
- the materiality of the correction;
- the length of time that has elapsed since the incorrect information was disclosed and the likelihood that it is still in active use by the third party;
- the number of entities that would need to be contacted by the agency or organisation; and

---

145 ANZ, *Submission PR 467*, 13 December 2007.
146 Acxiom Australia, *Submission PR 551*, 1 January 2008.
147 Law Council of Australia, *Submission PR 527*, 21 December 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007.
148 In Ch 25, the ALRC considers whether agencies and organisations should be required to log disclosures of personal information and comes to the view that the potential detriments associated with logging disclosures outweigh the potential benefits.
149 See Rec 29–9.

- the potential consequences for the individual of the use and disclosure of the incorrect information.

Recommendation 29–5 The 'Access and Correction' principle should provide that, if an individual seeks to have personal information corrected under the principle, an agency or organisation must take such steps, if any, as are reasonable to:

(a) correct the personal information so that, with reference to a purpose for which the information is held, it is accurate, relevant, up-to-date, complete and not misleading; and

(b) 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.

Annotation of disputed information

29.133 Where the correctness of personal information is the subject of dispute, the IPPs and the NPPs provide individuals with the right to have the information annotated.

29.134 The IPPs and NPPs, however, deal with this issue slightly differently. IPP 7 states that, in the event that there is a disagreement about correction, the record-keeper should 'attach' to the record, on request, any statement provided by the individual of the correction sought. On the other hand, NPP 6 requires the organisation, on request, to 'associate' with the information a statement that it is not accurate, complete or up-to-date. This raises the question of which approach is more appropriate. Should the obligation to annotate disputed information require an agency or organisation to attach a statement of the correction sought to the relevant record, or to 'associate' with the record the views of the individual concerned? For example, the Annotated National Privacy Principles state:

> It may be appropriate not to attach a statement where, for example, the relevant personal information is held in electronic format in template documents that have no capacity for attachments or where the statement is very lengthy.[150]

Submissions and consultations

29.135 In DP 72, the ALRC expressed the preliminary view that the wording in NPP 6.6 ('associate') was preferable to the wording in IPP 7 ('attach') because it was

150 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–4810].

more technology neutral. The ALRC was of the view that the use of the word 'associate' was more likely to achieve the main objective of the provision—namely, to ensure that the opinion of an individual about the correctness of his or her personal information is easily accessible when the organisation seeks to use or disclose the information.[151]

29.136 Optus supported the ALRC's view that the wording 'associate' was preferable, noting that the word 'attach' was technology specific and 'would be insupportable by virtue of the operation of some business systems'.[152] Privacy advocates also supported the suggestion that an organisation should associate with disputed information a statement claiming that the information is not correct, subject to the general requirement that any notes made about disputed information are apparent to subsequent users.[153]

ALRC's view

29.137 Agencies and organisations should be required to 'associate' with the record a statement of the correction, deletion or addition sought. This record should be associated in such a way that it is apparent to subsequent users. The ALRC considers this requirement to be inherent to the meaning of 'associate'. Currently, the OPC's *Information Sheet 4—Access and Correction* advises that:

> An organisation would ordinarily need to associate the individual's statement about the disputed information in such a way that whenever the information is handled in the future it will be easy to see that the individual is not satisfied that this particular part of the personal information is accurate, complete or up-to-date.[154]

29.138 In previous stages of this Inquiry, the ALRC considered the respective benefits of the word 'associate' only in the context of organisations. The policy reasons for adopting the word 'associate'—in particular, the term's technological neutrality—apply equally, however, to agencies and organisations. Accordingly, it is appropriate for this terminology also to apply to agencies.

Recommendation 29–6 The 'Access and Correction' principle should provide that an agency or organisation must, in the following circumstances, if requested to do so by the individual concerned, take reasonable steps to associate with the record a statement of the correction sought:

---

151 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [26.27]. As a result of the ALRC's approach to the reform of access and correction in DP 72, this view was raised only in the context of organisations.

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

153 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

154 Office of the Federal Privacy Commissioner, *Access and Correction*, Information Sheet 4 (2001).

(a) if the agency or organisation that holds personal information is not willing to correct personal information in accordance with a request by the individual concerned; and

(b) where the personal information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.

Procedural requirements for access and correction requests

29.139 Where an individual exercises his or her right to obtain access to, and correction of, personal information, the agency or organisation that holds the information must comply with a number of procedural requirements. For organisations, these requirements are set out in NPP 6. NPP 6.4, for example, limits the charge that an organisation can levy for providing an individual with access. NPP 6.7 requires an organisation to provide reasons for denial of access, or refusal to correct, personal information. The IPPs do not include equivalent procedural obligations. The *Plain English Guidelines to Information Privacy Principles 4–7*, however, note that, where an agency processes a request for access under the *Privacy Act*, it should comply with the administrative machinery set out in the FOI Act.[155]

29.140 In this section, the ALRC considers whether unified procedural requirements should apply to agencies and organisations and, if so, what should be the content of any such obligations. In particular, what requirements, if any, should apply to agencies and organisations:

- to minimise barriers associated with exercising access and correction rights; and
- for procedural fairness?

Unified procedural requirements for agencies and organisations?

29.141 As noted above, when processing requests for access to, and correction of, personal information under the *Privacy Act*, agencies generally are required to comply with the administrative processes set out in the FOI Act.[156]

---

155 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 13.

156 Ibid, 13.

29.142 In DP 72, the ALRC expressed the preliminary view that the *Privacy Act* should set out the procedure to be followed when dealing with a request to access or correct personal information held by agencies. The ALRC suggested that these procedures could be similar to, but less onerous than, those set out in the FOI Act, including:

- steps to be taken by an individual making an application for correction or annotation of personal information;
- the time to be taken to process a request to access or correct personal information;
- the transfer of a request to access or correct personal information to another agency;
- how personal information should be made available to the individual;
- how corrections should be made to personal information; and
- when incorrect information should be deleted.[157]

Submissions and consultations

29.143 Privacy NSW supported the proposal, provided the existing provisions in the FOI Act are referred to in the 'Access and Correction' principle itself or that these provisions be annexed to the *Privacy Act*.[158] The AFP supported the proposal and noted that the OPC should develop guidance in consultation with agencies.[159] The Public Interest Advocacy Centre (PIAC) submitted that procedures for correction should take into account a number of additional matters, including that, unless there is a very good reason to the contrary, individuals should always be given full access to the original record.[160] Medicare Australia agreed that the procedural details should be included in a new Part of the *Privacy Act*.[161]

29.144 The OPC submitted that the procedures to be followed should be clear, but noted that it was less convinced that all procedural matters needed be set out in legislation, as opposed to being subject to guidance. The OPC suggested that, where possible, the relevant provisions of the *Privacy Act* should mirror the proposed 'Access and Correction' principle for organisations. Where necessary, guidance could be issued by the OPC about certain procedures. In the OPC's view, only in circumstances where

---

157 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–11.
158 Privacy NSW, *Submission PR 468*, 14 December 2007.
159 Australian Federal Police, *Submission PR 545*, 24 December 2007.
160 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
161 Medicare Australia, *Submission PR 534*, 21 December 2007.

it is deemed essential should the prescriptive provisions of the FOI legislation be incorporated into the *Privacy Act*.[162]

ALRC's view

29.145 An individual seeking access to personal information held by an agency should not be subject to the FOI Act processes where a simpler process can be established. Providing agencies with the discretion afforded by principles-based provisions allows agencies to develop administrative processes that are simpler than those imposed under the FOI Act and are appropriate to that agency and the personal information that it holds.

29.146 It is appropriate, therefore, that procedures imposed on organisations under the 'Access and Correction' principle in the model UPPs also should apply to access to, and correction of, personal information held by agencies. The appropriate content for a number of procedural issues associated with access and correction is considered below.

Barriers to access and correction

Background

29.147 For individuals to exercise control over their personal information, access and correction rights—as well as being available in principle—must be meaningful in practice. The OECD Guidelines, for example, state that where an individual is entitled to access personal information about him or her, this should include the right to have it communicated:

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him …[163]

29.148 The NPPs include provisions addressing some of these barriers to access. Under NPP 6.4, if an organisation charges for providing access to personal information, the charges must not be excessive and must not apply to lodging a request for access. The OPC has advised that an organisation should take the following factors into account if it charges an individual for access to personal information: staff costs involved in locating and collating information; reproduction costs; and costs involved in having someone explain information to an individual. The OPC also has advised that

---

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

163 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 13(b).

an organisation should not charge an individual more than it costs the organisation to give access.[164]

29.149 Concern has been expressed, however, that a wide variety of fees may be charged for access to personal information because there is no maximum fee or schedule of fees in the *Privacy Act*. The OPC Review noted evidence of wide discrepancies in the fees charged by organisations for access to personal information and recommended that it should provide guidance to the private sector on fee structures.[165]

29.150 NPP 6 does not deal expressly with the remaining barriers to access set out in the OECD Guidelines—that is, that access to personal information should be provided within a reasonable time, in a reasonable manner, and in a form that is readily intelligible. This is in contrast to, for example, the *Health Records and Information Privacy Act 2002* (NSW), which provides that a request for access to health information must be responded to within 45 days of receipt.[166] Access also generally must be provided in the form requested by the individual.[167] Similarly, Victorian privacy law sets out specifically the timeframe within which a request for access to, or correction of, personal information must be acted upon.[168]

29.151 Arguably, NPP 6 can be interpreted to minimise some barriers to access. In *B v Surgeon*, for example, a patient brought a complaint about the form in which a surgeon offered to provide access to personal information. The Privacy Commissioner advised that—although NPP 6 does not specify the form in which access should be provided—'it is the Commissioner's view that access should generally be provided in the form requested by the individual'.[169]

29.152 The OPC also has suggested appropriate timeframes for access to personal information in its *Guidelines to the National Privacy Principles*. The Guidelines suggest the following response times, as a starting point for organisations:

---

164 Office of the Federal Privacy Commissioner, *Access and Correction*, Information Sheet 4 (2001).

165 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 31. See also rec 29, which provides that the Australian Government should consider adopting the Australian Health Ministers' Advisory Council Code as a schedule to the *Privacy Act*, which will address the issues of intermediaries and access fees. This is discussed further in Part H.

166 *Health Records and Information Privacy Act 2002* (NSW) s 27.

167 Ibid s 28. A private sector organisation may refuse to provide access to health information in the form requested by the individual if providing the information in that form would: place unreasonable demands on the organisation's resources; be detrimental to the preservation of the information or otherwise would not be appropriate; or involve an infringement of copyright.

168 See *Information Privacy Act 2000* (Vic) sch 1, IPP 6.8 (request to be actioned no later than 45 days after receipt).

169 *B v Surgeon* [2007] PrivCmrA 2. A patient lodged a complaint against a surgeon who would not provide the patient with a copy of his or her medical record. Rather, the surgeon offered for it to be viewed under the supervision of a staff member or provided to the complainant's surgeon of choice. Following the Privacy Commissioner's advice, the surgeon provided the complainant with copies of some of the medical records, excluding those documents that were considered commercially sensitive.

- If the individual has made a written request for access, acknowledging the request as soon as possible or at least within 14 days could, in many cases, be appropriate.
- If granting access is straightforward, it would often be appropriate for an organisation to grant access within 14 days, or if giving it is more complicated, within 30 days.[170]

29.153 The OPC notes, however, that the appropriate response time will depend on a number of factors, including

> The method of communication, the type or amount of personal information requested, how the personal information is held, how complex an organisation's functions and activities are and how the personal information is to be provided to the individual making the request.[171]

29.154 Some of these potential barriers to access also are provided for under the FOI Act's administrative machinery. For example, where an individual requests access in a particular form, agencies generally are required to comply with that request.[172] The FOI Act also sets out prescriptive timeframes within which agencies must respond to requests for access to personal information.[173]

Submissions and consultations

29.155 In DP 72, the ALRC proposed that the 'Access and Correction' principle should provide that an organisation must respond within a reasonable time to a request from an individual for access to personal information held by the organisation. The ALRC also proposed that the OPC should provide guidance about the meaning of 'reasonable time' in this context.[174]

29.156 The majority of stakeholders that commented on this issue supported the ALRC's proposal.[175] A number of stakeholders, however, suggested that there should be greater clarity about the timeframe for response.[176] The Office of the Victorian Privacy Commissioner (OVPC) suggested that the *Information Privacy Act 2000*

---

170 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 49.
171 Ibid, 49.
172 *Freedom of Information Act 1982* (Cth) s 20.
173 Ibid s 15.
174 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 26–3. The ALRC did not make an equivalent proposal in the context of agencies.
175 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
176 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

(Vic)—which requires Victorian agencies to respond as soon as is reasonably practicable, but by a maximum of 45 days—could provide an appropriate framework.

> This does not mean that the agency is required to have updated the personal information or even to have made a decision as to whether the information will be corrected within 45 days (although this may be the case). Instead, the agency is required to have responded to the request for access or correction within 45 days, and, ideally, to have provided a timeline for their response to the individual within that time.[177]

29.157 PIAC supported incorporating other aspects of the OECD Guidelines[178] into the 'Access and Correction' principle, including that the organisation should respond: in a reasonable manner; at a charge, if any, that is not excessive; and in a form that is readily intelligible to the individual. It suggested that the 'Access and Collection' principle should specify a maximum fee for access, or that a schedule of fees should be included in the regulations.[179] Privacy advocates also supported introducing binding benchmarks for fees.[180]

29.158 The OPC suggested that an organisation should be under an obligation to provide the personal information in the form requested by the individual, where practicable and reasonable. In addition, the form of access should

> have regard for any disability the individual may have, as well as their literacy and other matters, such as the individual's level of understanding of what the information relates to. For example, if the information is highly technical in nature and cannot be interpreted easily, the individual may request it in a translated form.[181]

ALRC's view

Fees

29.159 Currently, where an organisation imposes any charge for providing access to personal information, this charge must not be excessive and must not apply to lodging a request for access.[182] This provision should be included in the 'Access and Correction' principle.

29.160 Agencies presently are not permitted to charge an individual for providing access to personal information under the *Privacy Act*. The ALRC has not been made aware of any issues with agencies not being able to levy such a charge. In Chapter 32, the ALRC supports the general objective that individuals should not be unfairly

---

177 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

178 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 13(b).

179 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

180 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

182 *Privacy Act 1988* (Cth) sch 3, NPP 6.4.

disadvantaged by seeking to assert their privacy interests—and expresses the view that this requirement should be incorporated, where appropriate, into the privacy principles.

29.161 In light of the public interest in an individual being able to access and correct personal information that an agency holds about him or her, the ALRC considers that agencies should continue to fund the associated costs. The ALRC does not recommend, therefore, that the charging provisions should be extended to apply to agencies. This is consistent with the ALRC's conclusion in its Report, *Open Government* (ALRC 77), that access to one's own personal information under the FOI Act generally should be free.[183]

Timeliness of response

29.162 The 'Access and Correction' principle should include a requirement that agencies and organisations must respond to requests for access to personal information within a reasonable time. As responding to requests for access in a timely manner already may have been implied into the requirements of NPP 6 and has been recognised as 'best practice',[184] making this requirement explicit in the 'Access and Correction' principle will not require a change in practice for the vast majority of organisations. Further—as this requirement generally would not impose higher obligations on an agency than those timeframes required under the FOI Act—it also will not require a change in practice for agencies.

Manner of providing access

29.163 The 'Access and Correction' principle should require agencies and organisations to take reasonable steps to provide access in the manner requested by the individual. It is arguable that a requirement for organisations to provide access in the manner requested by the individual already can be implied into the 'Access and Correction' principle. This inference, however, is not self-evident. Expressly including a provision in relation to the manner of providing access therefore would promote clarity in the access and correction requirements. Such a provision also is consistent with present requirements for agencies under the FOI Act.

Generally understandable

29.164 In Chapter 10, the ALRC notes that it has not received evidence that indicates that information is being provided to individuals in an unintelligible form. The ALRC also considers it to be implicit within the concept of access that, where practicable, information should be provided in an intelligible form. The ALRC, therefore, does not

---

183 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [14.8].

184 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [7–3740].

recommend that the 'Access and Correction' principle should include a specific requirement for information to be provided in a form that is readily intelligible.

Level of detail of the provisions

29.165 There is a question of how prescriptive the procedural requirements in the 'Access and Correction' principle should be—for example, should the principle include maximum timeframes for responding to requests for access or a schedule of fees?

29.166 There are a number of practical difficulties with implementing binding schedules or frameworks in this context. For example, an appropriate timeframe to respond to an individual's request for access will depend on a myriad of factors.[185] It is therefore difficult to prescribe firm rules regarding the procedures to be followed when an individual seeks access to his or her personal information. Setting out the provisions to remove barriers to access as high-level principles, rather than in the form of prescriptive obligations, also is consistent with the ALRC's broader approach to privacy regulation.[186]

29.167 The ALRC recommends, below, that the OPC should develop guidance for agencies and organisations about their obligations under the 'Access and Correction' principle.[187] It is appropriate for the requirements to minimise barriers to individuals seeking to obtain access to, or correction of, personal information to be addressed in this guidance.

Recommendation 29–7 The 'Access and Correction' principle should provide that an agency or organisation must:

(a) respond within a reasonable period of time to a request from an individual for access to his or her personal information held by the agency or organisation; and

(b) provide access in the manner requested by the individual, where reasonable and practicable.

185 See Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 49. Similarly, the appropriate fee to charge for access will vary depending on the circumstances of the particular request.

186 See Chs 4 and 18.

187 Rec 29–9.

Reasons for decision and avenues of complaint

29.168 NPP 6.7 requires organisations to provide reasons for 'denial of access or a refusal to correct personal information'. It does not provide any further guidance on how reasons should be given, how detailed the reasons should be, or whether there are any circumstances in which reasons can be refused.

29.169 No limitations on the requirement to give reasons are included expressly in the provision. The Revised Explanatory Memorandum for the private sector provisions, however, states that NPP 6.7 generally will require an organisation to tell the individual which exception it is relying upon to refuse access.[188] Further, it states that an organisation would not be required to give reasons 'where such a disclosure would prejudice an investigation against fraud or other unlawful activity'.[189] The OPC also has issued guidance that:

> Where access is denied on the basis of a serious threat to life or health, [a health provider] need not specify the precise provision relied upon if they are concerned this would cause the very harm which the denial of access is meant to correct.[190]

29.170 The FOI Act provides that, where an agency has made a decision to refuse to grant access to a document, it must give notice in writing of the decision.[191] This notice is not required to contain any matter that is of such a nature that its inclusion would cause that document to be exempt under the Act.[192] By virtue of s 51D of the FOI Act, this requirement also applies to a decision to refuse to amend or annotate a record.

Submissions and consultations

29.171 Although no proposal was directed specifically to this issue, some stakeholders made submissions on the requirements for procedural fairness under the 'Access and Correction' principle.

29.172 Privacy advocates submitted that the obligation to give reasons needed to be more specific in requiring an organisation to specify *which* of the exceptions it has relied on to deny access or correction.[193]

29.173 The AGD noted that requiring organisations to provide a reason for the denial of access may prejudice investigations or prosecutions in relation to mutual assistance

---

188 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 151. See also *Acts Interpretation Act 1901* (Cth) s 25D.

189 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 151.

190 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), 4.

191 *Freedom of Information Act 1982* (Cth) s 26.

192 Ibid s 26(2).

193 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

or extradition. It suggested that there should be an exception from the requirement to provide a reason for denial of access where the reason for denial is because of one or more of paragraphs 9.1(f) to (j) of the proposed 'Access and Correction' principle.[194] The Department of Human Services questioned whether informal processes for providing reasons to deny a request to access personal information would be sufficient under the *Privacy Act*.[195]

29.174 The OVPC suggested that, where organisations decide to refuse access, they should be required to advise individuals about how this decision can be appealed.[196] Liberty Victoria expressed the view that individuals who are refused access to personal information should have an independent review process available to them.[197]

ALRC's view

29.175 Where an agency or organisation has made an adverse decision in relation to a request for access to personal information that it holds about an individual, or a decision to correct such information, it is an important element of procedural fairness for the individual to be provided with the reason for the adverse decision. This generally will require the agency or organisation to tell the individual which exception it is relying upon to refuse access. The process for providing reasons should be as informal as possible to ensure that reasons are given quickly and to reduce compliance costs.

29.176 There may be some situations, however, where providing reasons would undermine the very reason that the agency or organisation has denied the individual access to the information or has refused to make the requested correction. In these situations it may not be appropriate for reasons to be provided. The 'Access and Correction' principle should explicitly provide for these situations.

29.177 At the time that an individual is provided with an adverse decision relating to his or her right of access and correction, it is appropriate that the relevant agency or organisation provide that individual with information about the avenues of complaint or review. The ALRC recommends that agencies and organisations provide information about avenues of complaint available to an individual in their Privacy Policies. Provided this Privacy Policy is readily available, it would be open to an agency or organisation to meet its requirements under the 'Access and Correction' principle by referring individuals to the relevant section of this document.

---

194 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007. These exceptions are set out in paras 9.1(g)–(k) of the model 'Access and Correction' principle.

195 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

196 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

197 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.

Recommendation 29–8 The 'Access and Correction' principle should provide that where an agency or organisation denies a request for access, or refuses to correct personal information, it must provide the individual with:

(a) reasons for the denial of access or refusal to correct personal information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the personal information; and

(b) notice of potential avenues for complaint.

Notification of access and correction rights

29.178 The FOI Act requires agencies to publish information about the documents that are maintained by the agency and the facilities provided by the agency to enable individuals to access these documents.[198] There currently is no obligation under the *Privacy Act* or the FOI Act, however, to advise an individual that he or she may request the correction of his or her personal information where that individual has been given access to that information.[199]

29.179 In DP 72, the ALRC proposed that the *Privacy Act* should provide that, where an agency gives an individual access to personal information, it also must advise the individual that he or she may request the correction of that information.[200] The ALRC did not make an equivalent proposal for information held by organisations—rather, it suggested that the proposed 'Notification' and 'Openness' principles would cover adequately the notification requirements in this context.[201]

29.180 The OPC and Australia Post supported the ALRC's proposal.[202] The AFP supported the proposal in principle, on the basis that there would be appropriate exemptions to enable the AFP and other law enforcement agencies to properly perform all of their functions.[203] ACMA was concerned that the proposal may compromise the law enforcement and regulatory functions of agencies, and have resource implications.[204]

---

198 *Freedom of Information Act 1982* (Cth) s 8(1).
199 Such an obligation exists under Information Privacy Principle 6 of the *Privacy Act 1993* (NZ).
200 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–8(b).
201 Ibid, [26.60].
202 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.
203 Australian Federal Police, *Submission PR 545*, 24 December 2007.
204 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

ALRC's view

29.181 Agencies and organisations should take steps to inform individuals of their access and correction rights. This includes advising individuals who have obtained access to their personal information that they have the right to seek correction of this information. In the ALRC's view, however, this obligation does not need to be set out in the *Privacy Act*. Notification of access and correction rights is sufficiently encompassed by the ALRC's recommendation that, at or before the time that an agency or organisation collects personal information about an individual, it must take steps to make the individual aware of certain matters, including his or her rights of access to, and correction of, the information.[205]

Guidance on the 'Access and Correction' principle

29.182 The ALRC recommends a number of changes to the 'Access and Correction' principle. These changes impose new obligations on agencies and organisations, including an obligation to respond to a request for access in a timely manner and, in certain circumstances, to notify third parties of a correction to personal information. The ALRC recommends some changes to access and correction requirements to allow a unified 'Access and Correction' principle for agencies and organisations. Agencies and organisations will benefit from clear guidance on how these changes should be applied.

Recommendation 29–9 The Office of the Privacy Commissioner should develop and publish guidance on the 'Access and Correction' principle, including:

(a) when personal information is 'held' by an agency or organisation;

(b) the requirement that access to personal information should be provided to the maximum extent possible consistent with relevant exceptions;

(c) the factors that an agency or organisation should take into account when determining what is a reasonable period of time to respond to a request for access;

(d) the factors that an agency or organisation should take into account in determining when it would be reasonable and practicable to notify other entities to which it has disclosed personal information of a correction to this information; and

205 The 'Notification' principle is discussed in Ch 23.

(e) the interrelationships between access to, and correction of, personal information under the *Privacy Act* and other Commonwealth laws, in particular, those relating to freedom of information.

Summary of 'Access and Correction' principle

29.183 The ninth principle in the model UPPs should be called 'Access and Correction'. It may be summarised as follows.

UPP 9. Access and Correction

9.1 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, except to the extent that:

Where the information is held by an agency:

(a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or

Where the information is held by an organisation:

(b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;

(c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;

(d) the request for access is frivolous or vexatious;

(e) 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 in those proceedings;

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(g) providing access would be unlawful;

(h) denying access is required or authorised by or under law;

(i) providing access would be likely to prejudice an investigation of possible unlawful activity;

(j) providing access would be likely to prejudice the:

(i) prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) protection of the public revenue;

(iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.

9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it 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.

9.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.

9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.

9.6 If an agency or organisation holds personal information about an individual that is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:

(a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and

(b) 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.

9.7 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 and:

(a) the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant; and

(b) where the information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the agency or organisation must take reasonable steps to do so.

9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:

(a) reasons for the denial of access or refusal to correct the information, except to the extent that providing such reasons

would undermine a lawful reason for denying access or refusing to correct the information; and

(b) notice of potential avenues for complaint.

30. Identifiers

Contents

Introduction

30.1 Individuals are expected or required to identify themselves in a number of different contexts. For example, information about a person's identity is often disclosed in social situations and is often required in economic transactions. The purposes of identification are manifold. For example, identification can enable interpersonal and business relationships to develop, and reduce the possibility of criminal behaviour.

30.2 The type and quantity of evidence required to establish or verify a person's identity varies according to the context in which the identification is sought. Evidence of identity can include an assertion of a person's name, the appearance or characteristics of a person, a person's knowledge (such as a password) or the fact that a person is in possession of an object (such as a passport, birth certificate or card).[1] This chapter uses the term 'identifier' to refer to a number, symbol or some types of biometric information that uniquely identifies an individual for the purposes of an agency or organisation's operations.[2]

30.3 A number of objects that are given to individuals by agencies contain identifiers. Research conducted for the Office of the Privacy Commissioner (OPC) in 2004 revealed that the majority of Australians did not consider it an invasion of privacy to be asked to produce a document containing an identifier, such as a passport.[3]

30.4 In this chapter, the ALRC first considers whether the model Unified Privacy Principles (UPPs) should contain a separate principle to regulate identifiers and, if so, whether that principle should extend to the adoption, use and disclosure of identifiers by agencies. The ALRC then recommends changes to the content of the 'Identifiers' principle and the definition of the term 'identifier'. Finally, the ALRC makes recommendations for the regulation of multi-purpose identifiers such as tax file numbers (TFNs).

Current coverage by IPPs and NPPs

30.5 The Organisation for Economic Co-operation and Development *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines)[4] and the Information Privacy Principles (IPPs) do not contain a principle dealing explicitly with identifiers. On the other hand, the National Privacy Principles (NPPs) currently contain a principle (NPP 7) that deals specifically with identifiers.

---

1 R Clarke, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7(4) *Information Technology & People* 6, 10.

2 The definition of an 'identifier' is discussed later in this chapter.

3 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), [6.1].

4 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

30.6 NPP 7 defines an identifier as including 'a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations'. The principle regulates only the handling by organisations of identifiers assigned by agencies. An individual's name and Australian Business Number (ABN) are explicitly excluded from being considered identifiers for the purposes of the NPPs.

30.7 NPP 7.1 provides that an organisation must not adopt as its own identifier an identifier that has been assigned by an agency (or an agency's agent or contracted service provider).[5] NPP 7.2 provides that an organisation must not use or disclose an identifier assigned to an individual by an agency, an agency's agent or contracted service provider unless the use or disclosure:

- is necessary for the organisation to fulfil its obligations to the agency;
- falls under specified exceptions listed in NPP 2.1(e)–(h);[6] or
- is by a prescribed organisation of a prescribed identifier in prescribed circumstances.[7]

30.8 The combination of NPP 7.1A with the final exception creates a mechanism for the Governor-General to make regulations to prescribe an organisation that may adopt, use or disclose a prescribed identifier in prescribed circumstances, provided certain conditions are met. These conditions are set out in s 100 of the *Privacy Act 1988* (Cth). For example, s 100(2) requires that, before the Governor-General makes regulations that derogate from NPP 7, the minister responsible for administering the Act[8] needs to be satisfied that, in relation to the adoption, use or disclosure of the identifier: the agency that assigned the identifier agrees this is appropriate; the agency has consulted the Privacy Commissioner; and the derogation is for the benefit of the individual concerned.[9] These requirements do not apply in certain circumstances set out in s 100(3), namely if:

---

5 NPP 7.1A provides, however, that this prohibition does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

6 These exceptions are discussed in Ch 25.

7 The *Privacy (Private Sector) Regulations 2001* (Cth) prescribe a number of organisations, identifiers and circumstances for the purposes of NPP 7.2. See *Privacy (Private Sector) Regulations 2001* (Cth) regs 8–11.

8 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

9 In Ch 5, the ALRC discusses privacy regulations generally and recommends that the regulation-making power in the *Privacy Act* should be amended to provide that the Governor-General may make regulations, consistent with the Act, modifying the operation of the UPPs to impose different or more specific requirements, including imposing more or less stringent requirements, on agencies and organisations than are provided for in the UPPs: Rec 5–1.

> (a) the regulations prescribe an organisation, or class of organisations; and
>
> (b) the regulations prescribe an identifier, or class of identifiers, of a kind commonly used in the processing of pay, or deductions from pay, of Commonwealth officers, or a class of Commonwealth officers; and
>
> (c) the circumstances prescribed by the regulations for the use or disclosure by the organisation, or an organisation in the class, of the identifier, or an identifier in the class, relate to the provision by the organisation of superannuation services for the benefit of Commonwealth officers; and
>
> (d) before the regulations are made, the Minister consults the Commissioner about the proposed regulations.

30.9 To date, five exceptions have been made using the regulation-making mechanism in the *Privacy Act*.[10] For instance, the regulations provide that AvSuper is a prescribed organisation for the purposes of NPP 7.1A and:

> (b) the payroll number assigned to an individual by Airservices Australia or the Civil Aviation Safety Authority is a prescribed identifier; and
>
> (c) the prescribed circumstance is that the payroll number is adopted by AvSuper to provide a superannuation service to the individual.[11]

30.10 In addition to the mechanism in NPP 7.1A, the specified exceptions listed in NPP 2.1 allow an organisation to use or disclose an identifier assigned by an agency where:

- the organisation reasonably believes 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;[12]

- in the case of an individual's genetic information, the organisation reasonably believes the use or disclosure to a genetic relative of the individual is necessary to lessen or prevent a serious (but not necessarily imminent) threat to the life, health or safety of a genetic relative of the individual;

- the organisation has reason to suspect unlawful activity, and the use or disclosure is a necessary part of its reporting or investigation of the matter;

---

10 See *Privacy (Private Sector) Regulations 2001* (Cth) regs 7–11.

11 Ibid reg 7.

12 In Ch 25, the ALRC recommends that the 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety. See Rec 25–3 and accompanying text.

- it is required or authorised by law; and

- the organisation reasonably believes that the use or disclosure is reasonably necessary for certain specified functions of an enforcement body.[13]

30.11 The policy bases of the 'Identifiers' principle are twofold. First, NPP 7 was introduced 'to ensure that the increasing use of Australian Government identifiers does not lead to a de-facto system of universal identity numbers'.[14] Secondly, the regulation of identifiers reflects concern about the facilitation of data-matching by identifiers. Thus, NPP 7.1

> prevents an organisation from acquiring a particular government assigned identifier from all the individuals with which it deals and using that identifier to organise personal information it holds and match it with other personal information organised by reference to the same identifier.[15]

Is there a need for an 'Identifiers' principle?

30.12 A threshold issue is whether it is necessary to retain a separate principle to regulate the use of identifiers. There is an argument that the collection, use and disclosure of identifiers could be accommodated within the privacy principles that deal with those aspects of the information cycle. For example, the proscription in NPP 7 against the adoption by an organisation of an identifier assigned by an agency could be accommodated within the privacy principle governing use and disclosure of personal information.

30.13 A small number of submissions to the Issues Paper, *Review of Privacy* (IP 31) specifically addressed the question whether there should be a separate privacy principle to regulate the handling of identifiers.[16] Two stakeholders indicated that a separate principle was not required.[17] On the other hand, the Queensland Council for Civil Liberties supported the retention of 'a clear principle prohibiting the development of a universal or approaching universal identifier'.[18] The Office of the Information Commissioner (Northern Territory) was of the view that NPP 7 'currently performs a useful task in limiting the use of identifiers for data-matching and data-linkage'.[19] Further, the OPC noted that the current principle 'serves an important function in protecting information privacy'.

---

13 *Privacy Act 1988* (Cth) sch 3, NPP 7.2(b), which imports the exceptions to the use and disclosure prohibition in NPP 2.1(e)–(h).

14 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 269.

15 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [380].

16 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–26.

17 Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007.

18 Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

19 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

> A unique identifier can make it significantly easier to match or link personal information that has been collected in different contexts and for different purposes. Such linkages can facilitate a range of functions, such as more targeted (and potentially intrusive) direct marketing, through to data surveillance of how individuals go about their day to day lives.[20]

30.14 In Discussion Paper 72, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the UPPs should contain a separate principle that regulates identifiers.[21] The ALRC expressed the view that the policy bases for the 'Identifiers' principle remained relevant, and noted that it had not received feedback that indicated that the dangers associated with the possible misuse of identifiers could be dealt with more effectively by incorporating the provisions relating to identifiers in other privacy principles.[22]

30.15 The ALRC also proposed that the 'Identifiers' principle should not apply to the adoption, use or disclosure of a prescribed identifier by a prescribed organisation in prescribed circumstances.

Submissions and consultations

30.16 A number of stakeholders supported the retention of a separate privacy principle to regulate the handling of identifiers by organisations.[23] For example, the Public Interest Advocacy Centre (PIAC) submitted that the

> accommodation of identifiers within other privacy principles such as collection, use and disclosure would be unnecessarily complex, and would fail to give adequate recognition to the serious privacy risks associated with the misuse of identifiers.[24]

30.17 Other stakeholders accepted the policy bases for the 'Identifiers' principle, but expressed concern about the practical operation of the principle. The Association of Market and Social Research Organisations submitted that NPP 7 curtails practices that do not pose a threat to privacy and could have a public benefit. For example, 'in the market and social research industry, organisations are disinclined to carry out research involving Commonwealth Identifiers even on a double-blind basis'.[25] Centrelink submitted that:

> if restrictions similar to those currently in National Privacy Principle 7.2 are included in the UPPs, it would not allow for flexibility in service delivery to meet the agency's

---

20 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
21 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 27–1.
22 Ibid, [27.16].
23 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.
24 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
25 Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007.

> needs and our customers' expectations. Although NPP 7 allows for the making of regulations, the process is resource intensive.[26]

30.18 The Cyberspace Law and Policy Centre supported the existence of a separate principle, but did not agree with the proposed regulation-making exception. The Centre submitted that exceptions should be made through the public interest determination process as this will allow 'appropriate scrutiny and opportunities for public input which are not provided by a regulation-making power'.[27]

ALRC's view

30.19 There should be a separate 'Identifiers' principle. It is not desirable for organisations to refer to individuals by an identifier that is assigned by an agency, nor is it desirable to facilitate data-matching between agencies and organisations through the use of an identifier. A further benefit of a separate 'Identifiers' principle is that the principle can deal with issues unique to identifiers such as: the adoption of identifiers by organisations; the definition of the term; and the exceptions to the use and disclosure of identifiers by organisations.

30.20 As noted above, regulations can permit a prescribed organisation to adopt, use or disclose a prescribed identifier in prescribed circumstances. This ensures that the 'Identifiers' principle does not operate inflexibly to prevent an organisation from carrying out activities that have a public benefit or are essential to the operations of the organisation. This regulation-making mechanism should remain in the *Privacy Act.* This mechanism should conform to the regulation-making power recommended in Chapter 5 of this Report. As a consequence, the 'Identifiers' principle should require that the minister responsible for administering the *Privacy Act*[28] needs to be satisfied that the derogation from the privacy protection in the 'Identifiers' principle is for the benefit of the individual concerned.

30.21 The ALRC notes that the *Legislative Instruments Act 2003* (Cth) requires consultation, where practicable and appropriate, before the making of regulations and other legislative instruments.[29] Before the making of a regulation that derogates from the privacy protection contained in the 'Identifiers' principle, it would be practicable and appropriate for the Minister to consult with the Privacy Commissioner and the agency that assigned the identifier. The recommended changes to the 'Identifiers' principle, together with the consultation requirements in s 17 of the *Legislative*

---

26 Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

27 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. Public interest determinations are discussed in Ch 47.

28 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

29 *Legislative Instruments Act 2003* (Cth) s 17. Consultation particularly is required where the regulations are likely to have a direct or substantial indirect effect on business.

Instruments Act, addresses the requirements currently set out in s 100(2) of the *Privacy Act* and the exceptions to those requirements set out in s 100(3) of the Act.

30.22 The ALRC notes that the existing 'Identifiers' principle provides a number of other exceptions to the general prohibition against adopting, using or disclosing an identifier assigned by an agency (or its agent or contracted service provider). These exceptions allow use or disclosure of an identifier where the public benefit of the use or disclosure would outweigh consideration of individual privacy. For example, use or disclosure of an identifier could take place for the purposes of law enforcement.[30] In addition, the 'required or authorised by or under law' exception allows derogation from the 'Identifiers' principle to occur with full parliamentary scrutiny by the adoption or amendment of primary legislation.[31] If the derogation is deemed to be less significant, this can occur through the more expedited process of subordinate legislation, which still involves accountability measures, such as those provided for under the *Legislative Instruments Act*.

30.23 The exceptions to the 'Identifiers' principle provide sufficient flexibility to overcome any unwarranted impediments to the use of identifiers by organisations, while at the same time providing appropriate protection for the privacy rights of individuals.

Recommendation 30–1 The model Unified Privacy Principles should contain a principle called 'Identifiers' that applies to organisations.

Recommendation 30–2 The 'Identifiers' principle should include an exception for the adoption, use or disclosure by prescribed organisations of prescribed identifiers in prescribed circumstances. These should be set out in regulations made:

(a) in accordance with the regulations-making mechanism set out in the *Privacy Act*; and

(b) when the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

Application of 'Identifiers' principle to agencies?

30.24 Currently, agencies are not subject to a provision regulating the adoption, use and disclosure of identifiers. In contrast, some state and territory legislation regulates the assignment, adoption, use and disclosure of identifiers by public sector bodies.

30 See UPP 10.2(b) and UPP 5.1(f).
31 See UPP 10.2(b) and UPP 5.1(e).

Under this legislation, the assignment, adoption, use and disclosure of identifiers by public sector bodies is generally prohibited unless it is necessary for the body to carry out its functions efficiently, or if an individual consents to the use of their identifier.[32]

30.25 In IP 31, the ALRC asked whether agencies should be subject to an 'Identifiers' principle.[33] In DP 72, the ALRC identified support in submissions and consultations for making agencies subject to a privacy principle dealing with identifiers.[34] The ALRC expressed the preliminary view that the privacy and other risks associated with the adoption, use and disclosure of identifiers by organisations also apply in respect of agencies, and that further protection of identifiers is warranted. The ALRC proposed that the UPPs should contain a principle called 'Identifiers' that applies to both agencies and organisations,[35] noting that this approach would promote regulatory consistency between agencies and organisations.

Submissions and consultations

30.26 There was a divergence of views on this proposal. Privacy commissioners and privacy advocates supported the additional restrictions on the handling of identifiers by agencies.[36] In contrast, while some agencies provided in-principle support for the regulation of the handling of identifiers by agencies,[37] nearly all agencies expressed concern about the operation of the proposed 'Identifiers' principle.[38]

30.27 The OPC submitted that identifiers increased the likelihood of data-matching activities. Given the amount of personal information linked to identifiers issued by agencies, the risks associated with data-matching are also pertinent to data-matching

---

32 See *Information Privacy Act 2000* (Vic) sch 1, IPP 7.1; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7.1; *Information Act 2002* (NT) sch, IPP 7.1 (in relation to public organisations).

33 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–28.

34 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; K Pospisek, *Submission PR 104*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

35 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 27–1.

36 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

37 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

38 See, eg, Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Institute of Health and Welfare, *Submission PR 552*, 2 January 2008; Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007. See, however, Australian Bureau of Statistics, *Submission PR 383*, 6 December 2007.

programs conducted by agencies.[39] PIAC was 'concerned about the increasing number of identifiers being developed by government agencies as they strive to deliver services more efficiently and in a "joined-up government" manner'.[40] The Office of the Victorian Privacy Commissioner (OVPC) submitted that the 'Identifiers' principle proposed in DP 72 'addresses most directly the concerns behind the expression "just a number in a system"'.[41]

30.28 On the other hand, one stakeholder submitted that identifiers can be privacy enhancing in some circumstances:

> - Accurate identification ensures that the right information is associated with, communicated to, and accessed by, the right person; this is particularly important where information is stored and communicated electronically.
> - Identifiers may also replace identifying demographic details and then be used or disclosed in a non-identifying form for activities such [as] research, monitoring or analysis.[42]

30.29 The Attorney-General's Department (AGD) submitted that the proposed restrictions on the use and disclosure of identifiers by agencies could impede the operation of identity verification programs such as the National Document Verification Service (DVS).[43] 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. The DVS verifies with the document issuing agency the details, including any identifiers, on the face of the document. The DVS does not maintain a central data repository.[44]

30.30 The Department of Human Services submitted that 'it is imperative that any proposal regarding unique identifiers does not constrain [agencies'] ability to serve their customers efficiently and effectively'.[45] The Australian Taxation Office submitted that restrictions on the handling of identifiers by agencies could inhibit 'whole of government projects aimed at enabling people to register for interactions with government agencies more efficiently and with less repeating of information'.[46] The

---

39 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

40 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

41 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

42 Confidential, *Submission PR 570*, 13 February 2008. See also Australian Institute of Health and Welfare, *Submission PR 552*, 2 January 2008.

43 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

44 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.

45 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

46 Australian Taxation Office, *Submission PR 515*, 21 December 2007.

Department of Finance and Deregulation suggested that such concerns are particularly pertinent for individuals transacting with agencies in the online environment.[47]

30.31 The Australian Institute of Health and Welfare was concerned that the proposed extension of the 'Identifiers' principle would restrict the use and disclosure of identifiers for research purposes.

> Statistical linkage keys (SLKs), which appear to fall within the proposed definition of identifiers, have been implemented in many national information collections to enable the linkage of data for statistical and research purposes, not for administrative purposes … The use of a SLK enables the development of a person-based view (rather than episode-based view) without using identifiable personal data; it is therefore a privacy preserving technique. This is particularly important for developing a whole of government, person-based approach to the planning and delivery of services.[48]

30.32 Some stakeholders suggested that, if the ALRC were to recommend that the 'Identifiers' principle be extended to regulate agencies, the ALRC should also recommend that the principle include an exception that would allow an individual to consent to the use and disclosure of their identifier.[49] The Department of Finance and Deregulation noted

> the concerns expressed in the Discussion Paper around 'bundled consent', where an individual may be coerced into consenting to the disclosure of their personal information or to some other sacrifice of privacy rights to gain a particular benefit. While acknowledging that is a serious concern in the commercial sector, Finance does not consider that a citizen choosing to use one agency identifier to transact with other agencies constitutes 'bundled consent'.[50]

30.33 Finally, Medicare Australia submitted that 'the real issue is not the identifier itself, but what happens to the information attached to the identifier—ie the risks associated with uncontrolled data matching'. Medicare Australia was of the view that regulation of identifiers should focus more directly on these risks, rather than restriction of the use of identifiers. This was especially the case 'given that those restrictions are currently impeding the efficient administration of both agencies and organisations'.[51]

---

47 Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008.

48 Australian Institute of Health and Welfare, *Submission PR 552*, 2 January 2008.

49 Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

50 Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008.

51 Medicare Australia, *Submission PR 534*, 21 December 2007.

ALRC's view

30.34 The policy objectives underlying the recommended 'Identifiers' principle—preventing an identifier that is assigned by an agency from becoming a de facto national identity number, and restricting the use of an identifier to facilitate data-matching programs—are also relevant to the handling of identifiers by agencies. In addition, making agencies subject to the 'Identifiers' principle would promote regulatory consistency. The ALRC agrees, however, that applying the 'Identifiers' principle to agencies could seriously impede activities conducted for a public benefit, including: programs designed to reduce fraud and identity theft; service delivery; and research.

30.35 The feedback received by the ALRC indicates that appropriate and important information sharing between agencies would be restricted by the application of the 'Identifiers' principle.[52] It does not follow, however, that the handling of identifiers by agencies should not be regulated. The privacy principles dealing with collection, use and disclosure of personal information provide some regulation of the handling of identifiers by agencies. Given the privacy risks associated with identifiers, however, additional restrictions on the handling of identifiers by agencies will sometimes be appropriate.

30.36 One solution could be an 'Identifiers' principle that regulates the handling of identifiers by agencies, subject to several agency-specific exceptions.[53] While this approach might provide a better balance between activities conducted by agencies for a public benefit against the protection of individual privacy, it would lead to greater complexity of regulation in this area. Further, this approach may require the introduction of numerous agency-specific exceptions and, accordingly, may not be the most effective approach to regulation. Nor is this approach consistent with the ALRC's high-level, outcomes-based approach to privacy regulation.[54]

30.37 A better approach is to regulate the assignment, collection, adoption, use and disclosure of identifiers by agencies on a case-by-case basis. This could be carried out either in separate sectoral legislation or guidance provided by the OPC. Such an approach has been taken to the regulation of TFNs,[55] and was the approach taken in the development of the access card scheme.[56] The ALRC also notes that agencies currently are subject to data-matching guidelines issued by the OPC.[57]

---

52 In Ch 14, the ALRC makes a number of recommendations related to information sharing practices of agencies.

53 One such exception could allow an individual to consent to the adoption, use or disclosure of his or her identifier in certain circumstances. Another exception could allow identifiers to be used and disclosed by agencies for the purposes of research.

54 The ALRC's approach to privacy regulation is discussed in Chs 4 and 18.

55 TFNs are discussed later in this chapter.

56 See, eg, Human Services (Enhanced Service Delivery) Bill 2007 (Cth).

57 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998).

30.38 Many of the privacy risks associated with identifiers are heightened by the use of multi-purpose identifiers. In this chapter, the ALRC makes recommendations directed towards the regulation of such identifiers.[58]

Definition of 'identifier'

30.39 The definition of an 'identifier' in NPP 7 does not describe what an identifier is, only that it includes a number assigned by an organisation to an individual. The OPC *Guidelines to the National Privacy Principles*, however, set out a definition of 'identifier':

> A Commonwealth government identifier is a unique combination of letters and numbers, such as a Medicare number, which Commonwealth government agencies or contracted service providers allot to an individual.[59]

30.40 In DP 72, the ALRC considered whether the definition of an 'identifier' should include: identifiers that are not technically unique; identifiers containing biometric information; and an individual's name and ABN.

Unique

30.41 The current definition of 'identifier' requires that it 'identify uniquely the individual for the purposes of the organisation's operations'.[60] The OVPC submitted that some identifiers issued by agencies are not in fact 'unique'.[61] For example, Medicare numbers are listed as an example of a unique identifier in Guidelines issued by the OPC.[62] In circumstances where two or more family members share a Medicare number, however, the number does not, of itself, uniquely identify each of those family members.[63]

30.42 Secondly, while a biometric characteristic is generally unique to an individual, it is important to note that a number of factors may affect whether a biometric system can produce an exact match between a biometric sample and a stored template. For example, the quality of a collected sample, such as a facial image, may be affected by lighting conditions, camera distance and lens precision. The accuracy of the match may also be affected by 'the losses introduced by the extraction of biometric features such as face geometry, and the availability of comparative biometric data from the general population'.[64]

---

58 Recs 30–6 and 30–7.
59 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 55.
60 *Privacy Act 1988* (Cth) sch 3, NPP 7.3.
61 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.
62 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 55.
63 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.
64 M Wagner, *Correspondence*, 16 April 2007.

30.43 In DP 72, the ALRC proposed that the OPC be empowered to make a determination that, where a number, symbol or other particular does not, of itself, uniquely identify an individual, that number, symbol or particular is still an 'identifier' for the purposes of the 'Identifiers' principle.[65] Further, the ALRC proposed that the 'Identifiers' principle should contain a note stating that a determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act*.[66]

Submissions and consultations

30.44 The OPC queried whether the proposed determination-making power was necessary. The OPC submitted that the ALRC's expanded definition of an 'identifier' to include a number, symbol or any other particular, would seem to provide for future contingencies.[67] On the other hand, the OVPC supported the proposed determination-making power, submitting that this would provide an avenue for regulating identifiers that are not actually unique, such as Medicare numbers.[68]

30.45 PIAC was concerned that the proposed determination-making power provided 'too broad a discretion to the OPC and that any determinations by the OPC are liable to be disallowed by the Australian Parliament in any event'.[69]

ALRC's view

30.46 The definition of an 'identifier' requires it to 'identify uniquely' an individual. A determination-making power of the kind proposed in DP 72 will allow the Privacy Commissioner to determine that identifiers that are not actually 'unique', such as a shared Medicare number, still are identifiers for the purpose of the 'Identifiers' principle.[70] The ALRC notes that the OPC's submission is directed towards the types of information that could be an identifier, rather than the situation where an identifier is not unique to the assigning agency.

30.47 In addition, a determination-making power would deal with possible ambiguities about whether personal information is an 'identifier'. The ALRC anticipates, however, that such a determination would rarely be required. The recommended definition of 'identifier', therefore, should not place a significant burden on the Privacy Commissioner. Further, the definition of 'identifier' should include a note stating that a determination referred to in the recommended 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth). The

---

65 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 27–2.
66 Ibid, Proposal 27–3.
67 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
68 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
69 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
70 The ALRC notes that, if the recommendations in Ch 3 are implemented, such a determination could apply in state and territory jurisdictions. In addition, in Ch 17, the ALRC recommends that the OPC should develop and publish memoranda of understanding with each of the bodies with responsibility for information privacy in Australia, including state and territory bodies: Rec 17–3.

inclusion of this note clarifies that any determination made by the Privacy Commissioner may be disallowable by the Australian Parliament. The ALRC remains of the view that this is an appropriate check on the discretion afforded to the Privacy Commissioner.

Biometric information

30.48 Biometric information relates to the physiological or behavioural characteristics of a person.[71] Throughout this Inquiry, the ALRC has noted the privacy risks associated with the handling of this information.[72] In particular, the sensitive and permanent nature of biometric information has led the ALRC to recommend that the definition of 'sensitive information' be amended to include biometric information collected for certain purposes.[73]

30.49 Biometric information can be used as an identifier. An example of a biometric identifier used by agencies is the Australian ePassport that was introduced in 2005. The Australian ePassport includes a digital photograph of the passport holder on a chip embedded in the centre page of the passport.[74]

30.50 The current definition of 'identifier' in NPP 7 does not exclude specifically biometric information. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states that identifiers are 'not limited to letters and numbers' although an identifier 'will often contain either, or both'.[75] Biometric identifiers that are not stored in an encrypted form, therefore, are probably included in the current definition. Nonetheless, to ensure that biometric and other non-numerical identifiers are regulated by the 'Identifiers' principle, the ALRC proposed in DP 72 that an identifier should include 'a number, symbol or any other particular'.[76]

---

71 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.
72 The privacy risks associated with biometric systems technology are discussed in Ch 9.
73 Rec 6–4.
74 A Downer (Minister for Foreign Affairs), 'Australia Launches ePassports' (Press Release, 25 October 2005).
75 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 147.
76 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 27–2.

Submissions and consultations

30.51 A number of stakeholders supported this proposal.[77] Privacy NSW suggested that the definition of an 'identifier' should make 'overt reference' to biometric information to make clear that this information is an identifier.[78]

30.52 On the other hand, the AGD had two concerns about the broadening of the definition of an 'identifier'. First, it stated that the proposed inclusion in the definition of 'sensitive information' of certain types of biometric information

> creates an anomaly as biometric information could be collected as 'sensitive information' with consent under proposed UPP 2.6, but not used or disclosed as an 'identifier' with consent under proposed UPP 10.4.[79]

30.53 Secondly, the AGD submitted that a biometric algorithm—or identifier—that is generated when a person enrols in a biometric system is not unique to the agency or organisation assigning the identifier. In the AGD's view, this means that proscribing the adoption, use or disclosure of an identifier assigned by one agency is unworkable, as this identifier will be independently generated by a number of agencies.[80]

30.54 The Cyberspace Law and Policy Centre submitted that the 'definition of "identifier" should also encompass when identifiers are used for authentication (verification) and not only when used for identification'.[81]

ALRC's view

30.55 Some types of biometric information should be included in the definition of an 'identifier'. The ALRC agrees, however, that the words 'or any other particular' in the proposed definition of an 'identifier' potentially include a large amount of non-sensitive personal information. In the ALRC's view, the definition of an 'identifier' should reflect the specific concern about biometric information.

30.56 Explicit protection of some types of biometric information is warranted where this information is used as an identifier assigned by an agency and adopted, used or

---

77 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; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. Two stakeholders did not oppose the proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

78 Privacy NSW, *Submission PR 468*, 14 December 2007.

79 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007. In Ch 6, the ALRC recommends that the definition of 'sensitive information' should be amended to include: biometric information collected for the purpose of automated biometric authentication or identification; and biometric template information: Rec 6–4.

80 Ibid.

81 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

disclosed by an organisation. The ALRC notes the particular privacy risks associated with the handling of an individual's biometric information.[82] Further, the policy bases underlying the 'Identifiers' principle also are relevant for biometric identifiers. The 'Identifiers' principle contains a number of exceptions that would allow organisations to use or disclose such biometric information—for example, where such use or disclosure is required or authorised by or under law, or where regulations allow the handling of certain identifiers in certain circumstances. As discussed later in this chapter, any unique multi-purpose identifier that contains biometric information should be regulated by separate, sectoral legislation that addresses the specific privacy risks and concerns associated with such a scheme.

30.57 The AGD submitted that it is technically possible for separate biometric systems to generate identical biometric templates of the same individual. The OPC should make clear in guidance that agencies and organisations that design or deploy biometric systems technology should ensure the unique nature of the biometric templates issued by the systems. As noted above, the OPC should be empowered to make a determination to ensure that, where a number, symbol or certain type of biometric information does not of itself uniquely identify an individual, that number, symbol or biometric information is still an 'identifier' for the purposes of the 'Identifiers' principle.

30.58 Finally, the ALRC agrees that the definition of an 'identifier' also should refer to identifiers that are assigned by an agency to verify the identity of an individual. This is particularly pertinent in the context of biometric systems, where certain biometric identifiers assigned to an individual only will be used by an agency for the purpose of identity verification—for example, at a national border to verify that an individual is who his or her passport states that he or she is.

Individual's name and ABN

30.59 NPP 7.3 excludes an individual's name and ABN from the definition of an 'identifier'. NPP 7.3 provides that an ABN has the meaning given to it in the *A New Tax System (Australian Business Number) Act 1999* (Cth). This Act provides that an

> ***ABN (Australian Business Number)*** for an entity means the entity's ABN as shown in the Australian Business Register.[83]

30.60 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) explains why an ABN was expressly excluded from the definition in NPP 7.

> An ABN, intended to be a unique business identifier, may, where assigned to a sole trader, also identify an individual. The restrictions on using identifiers assigned by

82 The privacy risks associated with biometric systems technology are discussed further in Ch 9.
83 *A New Tax System (Australian Business Number) Act 1999* (Cth) s 41.

> agencies are not intended to apply within the context of the ABN scheme. For this reason an ABN is specifically excluded from the definition of 'identifier'.[84]

30.61 In DP 72, the ALRC expressed the view that, for the avoidance of doubt, an individual's name and ABN should continue to be excluded expressly from the definition of 'identifier'.[85]

Submissions and consultations

30.62 The ALRC received limited feedback about whether it remains appropriate to exclude an individual's name or ABN from the definition of 'identifier'. One submission supported specifically the continued exclusion of an ABN from the definition.[86]

ALRC's view

30.63 NPP 7 regulates the handling of identifiers assigned to individuals—not identifiers assigned to organisations. 'Individual' is defined in the *Privacy Act* to mean a natural person.[87] An 'organisation' includes an individual who acts in a business capacity, such as a sole trader.[88] The exclusion of an ABN from the definition of 'identifier' may be a problem if there is a tendency among organisations or agencies to use the ABN of a sole trader to identify an individual acting in a non-business capacity. The ALRC has not received information about such practices, however, and is of the view that the exclusion of an ABN from the definition of an 'identifier' is appropriate.

30.64 No stakeholder suggested that the definition of 'identifier' should be amended to include an individual's name. An individual's name is not assigned by an agency. The ALRC is of the view that, for the avoidance of doubt, an individual's name and ABN should continue to be excluded from the statutory definition of 'identifier'.

Recommendation 30–3 The 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

(a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or

(b) is determined to be an identifier by the Privacy Commissioner.

---

84 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [383].
85 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 27–2.
86 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
87 *Privacy Act 1988* (Cth) s 6(1).
88 Ibid ss 6C, 7B, 16E.

However, an individual's name or Australian Business Number, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

Recommendation 30–4 The 'Identifiers' principle should contain a note stating that a determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth).

Content of privacy principle dealing with identifiers

Use and disclosure for the purpose of identity verification

30.65 An issue that arose in response to DP 72 was whether the proposed 'Identifiers' principle would prevent an agency or organisation from using or disclosing an identifier for the purpose of identity verification.[89] The AGD submitted that:

> Identifiers are critical for the operation of identity management and an essential feature for identifying documents and credentials … any regulation of identifiers should put it beyond doubt that the use or disclosure of identifiers to enable an agency or organisation to establish or verify a client's identity for a lawful purpose is allowed.[90]

30.66 Smartnet commented further on the concerns about identity verification:

> Australia has no real system of identity or identity protection … there is a tendency for organisations (both government and private) to repeatedly ask us to re-establish our identity on each occasion we deal with them. While this is seen by some to be 'privacy enhancing' it does tend to create unnecessary and undisciplined holdings of personal information throughout business, government and the community. As a result, none of us has any idea of what has been collected or where it has ended up.[91]

30.67 As noted above, the ALRC has not recommended that agencies be made subject to the 'Identifiers' principle. Before considering whether amendment to the regulation of the handling of identifiers by organisations is required in light of the above submissions, the ALRC makes two key observations. First, the 'Identifiers' principle does not regulate the situation where an identifier is merely sighted by an organisation,

---

89 See, eg, Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008; Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Smartnet, *Submission PR 457*, 11 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.

90 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

91 Smartnet, *Submission PR 457*, 11 December 2007.

rather than collected for inclusion in a record and then used or disclosed by that organisation. For example, an individual purchasing alcohol from a bottleshop may be required to show a document such as a proof-of-age card or driver's licence that verifies that he or she is at least 18 years of age. The ALRC does not suggest that the practice of an organisation sighting an identifier contained on such a card or driver's licence should be regulated under the 'Identifiers' principle.

30.68 Secondly, there is a difference between identification (determining who an individual is), and verification or authentication (verifying that an individual is who or what he or she claims to be). In the example above, the bottleshop was required to verify that the individual purchasing alcohol was at least 18 years of age—the bottleshop did not need to identify the individual.[92] It is to the concept of identification that the stringent regulation in the 'Identifiers' principle is directed.

30.69 In the online environment, appropriately designed verification or authentication frameworks can be privacy enhancing. This is reflected in the *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* (2007). In the Preface to the Recommendation, the OECD Council stated:

> Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of trust relationships for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to protect information systems and networks, financial data, personal information and other assets from unauthorised access or identity theft. Electronic authentication is therefore essential for establishing accountability online.[93]

30.70 The ALRC notes that the Australian Government is developing an authentication framework that aims 'to enable e-government by providing confidence in online transactions with government'.[94]

ALRC's view

30.71 The use or disclosure of an identifier by an organisation for the sole purpose of verifying the identity of a person is not inconsistent with the policy basis of the 'Identifiers' principle. Organisations frequently require an individual to establish their identity prior to entering into any transactions. This situation is not always set out in legislation or rules in a way that clearly meets the 'required or authorised by law' exception in the 'Identifiers' principle. Such a use or disclosure does not permit the organisation to adopt that identifier for its own purposes. Secondly, such a use or

---

92 This distinction is discussed further in Ch 9, and informs the wording of the ALRC's recommendation to amend the definition of 'sensitive information' in Ch 6.

93 Organisation for Economic Co-operation and Development, *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* (2007), 7.

94 Australian Government Information Management Office, *ICT Infrastructure—Authentication* (2008) <www.agimo.gov.au/infrastructure/authentication> at 31 March 2008.

disclosure does not permit secondary use or disclosure for the purposes of data-matching.

30.72 It would not be desirable for the 'Identifiers' principle to prevent organisations from merely verifying an individual's identity by collecting, using and disclosing the identifiers contained within a high-integrity document, such as a birth certificate or Australian Government passport. In the event that the 'Identifiers' principle inhibits temporary handling of identifiers for the purposes of verification, rather than identification, the OPC could develop and publish guidance that addresses the issue.

Data-matching

30.73 In IP 31, the ALRC asked whether the identifiers principle should be redrafted to deal more generally with data-matching.[95] Submissions to IP 31 indicated support for greater regulation of data-matching. A number of submissions expressed concern about the extent to which agencies and organisations could use identifiers to facilitate data-matching processes.[96]

30.74 Several stakeholders pointed out, however, that data-matching programs are not conducted solely by use of identifiers. For example, the OVPC noted that data-sets may be linked through the use of names and dates of birth.[97] Similarly, the CSIRO submitted that 'two databases with sufficiently many data fields in common can be matched using well-developed data linkage techniques'.[98]

30.75 In DP 72, the ALRC expressed the preliminary view that data-matching should not be regulated by the 'Identifiers' principle.[99]

ALRC's view

30.76 Data-matching is not inherently linked to the use of identifiers. While the 'Identifiers' principle provides some regulation of data-matching, in that it prohibits the adoption by an organisation of an individual's identifier, other than for a specified purpose, data-sets can be linked by an organisation's use of information that will not be subject to this principle. Data-matching activities, therefore, should be subject to

---

95 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–26. The impact of data-matching on privacy is discussed in Chs 9 and 10.

96 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; CSIRO, *Submission PR 176*, 6 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

97 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

98 CSIRO, *Submission PR 176*, 6 February 2007.

99 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [27.50]. The Cyberspace Law and Policy Centre agreed with this view in its submission to DP 72: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

regulation separate to this principle. In Chapter 10, the ALRC recommends that the OPC should develop and publish guidance for organisations on the privacy implications of data-matching.[100]

Collection of identifiers

30.77 Submissions to the OPC Review of the private sector provisions of the *Privacy Act* (OPC Review) expressed concern about the collection of identifiers by organisations seeking to establish evidence of identity.[101] For example, individuals may be asked to present a Medicare card, an Australian passport or a document with a Centrelink reference number, and such documents may be photocopied by the organisation. NPP 7 does not prohibit the collection of identifiers. The OPC stated that there does not appear to be a need specifically to prohibit the collection of Australian Government identifiers because the collection of identifiers into a record is regulated by NPP 1:

> [I]f an identifier is collected by an organisation, but cannot be lawfully used or disclosed pursuant to NPP 7.2, then the collection is not necessary for one of the organisation's functions or activities. As a consequence, the collection would be prohibited by NPP 1.1.[102]

30.78 In DP 72, the ALRC agreed that the current regulation of the collection of identifiers was appropriate. There was limited feedback on this issue.[103]

ALRC's view

30.79 Both the IPPs and NPPs currently provide that an agency or organisation should only collect personal information that is necessary for it to carry out its functions or activities.[104] This requirement will form part of the 'Collection' principle in the model UPPs.[105] Where the collection of an identifier is not reasonably necessary for an agency or organisation to carry out its functions or activities, that collection will not be permitted and will constitute an 'interference with the privacy of an individual'.[106] Such requirements are adequate.[107]

Assignment of identifiers

30.80 Neither NPP 7 nor the IPPs regulate the *assignment* of identifiers by agencies. The process of 'assignment' involves an entity (such as an agency) choosing an identifier to apply to an individual. For example, an agency may assign an identifier,

---

100 Rec 10–4.
101 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 270.
102 Ibid, 272.
103 The Cyberspace Law and Policy Centre supported the ALRC's preliminary view in DP 72: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
104 *Privacy Act 1988* (Cth), IPP 1.1(b), NPP 1.1.
105 Rec 21–5.
106 *Privacy Act 1988* (Cth), ss 13 and 13A.
107 The powers of the OPC to deal with interferences with privacy are discussed in Part F.

consisting of a combination of letters and numbers, to each individual to whom it provides a service. The agency would then, in its records, refer to each of those individuals by the identifier it has assigned. This should be distinguished from *adopting* an identifier, which involves an agency or organisation using an identifier that has already been assigned by another agency to refer to an individual.

30.81 Certain state and territory provisions go further than the NPPs and IPPs by regulating the assignment of identifiers—either by agencies, organisations or both.[108] There is a gap, therefore, in the federal privacy principles in that they do not regulate the assignment of identifiers.

30.82 In DP 72, the ALRC asked whether the *Privacy Act* should regulate the assignment of identifiers by agencies, organisations or both.[109]

Submissions and consultations

30.83 Some stakeholders supported the regulation of the assignment of identifiers by agencies and organisations.[110] The OPC submitted that this

> would encourage good privacy practice by agencies, by creating a compliance culture in which these agencies consider the necessity of assigning an identifier for their functions and activities.[111]

30.84 On the other hand, the majority of agencies that responded to this question were opposed to the regulation of the assignment of identifiers. For example, Medicare Australia submitted that regulation of identifiers that are issued by agencies for internal use would 'add a level of complexity and bureaucracy which is not warranted'.[112] Some organisations also opposed the regulation of the assignment of identifiers. GE Money Australia queried whether identifiers assigned by organisations had been the subject of significant criticism.[113] One individual suggested that such regulation would be better directed towards the use and disclosure of an identifier for the purposes of data-matching.[114]

---

108 See *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7.1 (applicable to public and private sector organisations); *Information Act 2002* (NT) sch, IPP 7.1 (applicable to public sector organisations); *Information Privacy Act 2000* (Vic) sch 1, IPP 7.1.

109 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 27–1.

110 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. Another stakeholder submitted that it had no objections to such regulation: National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

112 Medicare Australia, *Submission PR 534*, 21 December 2007. See also Confidential, *Submission PR 570*, 13 February 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

113 GE Money Australia, *Submission PR 537*, 21 December 2007. See also Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; AXA, *Submission PR 442*, 10 December 2007.

114 P Youngman, *Submission PR 394*, 7 December 2007.

ALRC's view

30.85 The privacy risks associated with an identifier arise when that identifier is inappropriately adopted, used or disclosed, rather than when it is assigned. Agencies and organisations frequently assign identifiers solely for the internal use of the agency or organisation. The ALRC agrees that the regulation of the assignment of identifiers would add unwarranted complexity to the 'Identifiers' principle.

30.86 The ALRC does not recommend that the 'Identifiers' principle regulate agencies. Nonetheless, the ALRC agrees with the OPC that an agency should consider the necessity of the assignment of an identifier, particularly where that identifier might be adopted, used or disclosed by another agency. The ALRC makes a recommendation to address the concerns about multi-purpose identifiers later in this chapter.[115]

Consent to the use and disclosure of identifiers

30.87 NPP 7 does not provide for an exception to the use, disclosure or adoption of unique identifiers based on the consent of an individual. Some states and territories do provide for such an exception. These jurisdictions, however, do not have regulation-making powers comparable to those contained in the 'Identifiers' principle.[116]

30.88 In DP 72, the ALRC expressed the view that it would be inconsistent with the function of the 'Identifiers' principle to include an exception that allows an individual to consent to the use, disclosure or adoption of his or her identifier.[117] The ALRC noted that other legislation, or regulations issued under s 100 of the *Privacy Act*, can provide for circumstances where the Australian Parliament considers it appropriate for an individual to be able to consent to the use or disclosure of his or her identifier.[118]

Submissions and consultations

30.89 Centrelink submitted that the restriction on the use or disclosure of identifiers impedes the operation of a number of its existing services, which provide information to organisations about the concessional status of the individual with the consent of the individual concerned. These 'online, real time' services save time for both individuals and organisations. Centrelink submitted that the process of making regulations to prescribe such identifiers was resource intensive.[119]

30.90 The OPC, on the other hand, expressed concern about the unintended effects on privacy that could result from including a broad consent exception to the identifiers principle:

---

115 Rec 30–6.

116 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPPs 7.2(b), 7.3(c); *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7(2)(b); *Information Act 2002* (NT) sch, IPPs 7.2(b), 7.3(b).

117 Consent is discussed further in Ch 19.

118 See also *Privacy Act 1988* (Cth) sch 3, NPP 7.2(b).

119 Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

> the privacy risks of sharing unique identifiers are not always immediate. The risks accumulate as more organisations or agencies adopt the number for their own purposes, and as greater amounts of otherwise unrelated personal information become associated with that number. Accordingly, individuals may not always be conscious of the inherent risks of consenting to incrementally greater uses of their unique identifier.[120]

30.91 The OPC also expressed concern about 'bundled consent'.

> In some circumstances consent to a particular information-handling practice may be an imperfect form of privacy protection … Bundled consent is often sought as part of the terms and conditions of a service. In the context of a unique identifier, consenting to it being handled in certain ways may be bundled as a condition of service.[121]

ALRC's view

30.92 It would be convenient for an individual to be able to consent to the use or disclosure of his or her identifier by an organisation in certain circumstances.[122] The ALRC agrees with the OPC, however, that the privacy risks associated with identifiers are not immediate. On balance, a general consent exception would significantly reduce the protection afforded by the 'Identifiers' principle. In addition, the prescription of certain identifiers as specific exceptions listed within the 'Identifiers' principle does not accord with the high-level outcomes-based approach to privacy regulation followed by the ALRC in this Inquiry.[123]

30.93 In specific circumstances, it could be appropriate for an individual to consent to the handling of a specific identifier by a specific organisation. In such cases, it is preferable for separate primary or subordinate legislation to be enacted to allow individuals to consent to such specific handling—for example, existing regulations allow an individual to consent to the disclosure of his or her Centrelink Customer Reference Number[124] by certain organisations for the purpose of confirming that individual's concessional status with Centrelink.[125]

Identifiers issued by state and territory agencies

30.94 NPP 7.1 currently prevents an organisation from adopting as its own identifier an identifier that has been assigned by an Australian Government agency; an agent of that agency; or a contracted service provider of an Australian Government agency. Identifiers issued by state and territory agencies—for example, driver's licence numbers—do not fall within the current definition of 'identifier' in NPP 7.

---

120 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. The OPC provided the example of the widespread use and disclosure in Canada of the Canadian Social Insurance Number.

121 Ibid.

122 Note that the ALRC has not recommended that the 'Identifiers' principle apply to agencies.

123 The ALRC's approach to regulation is discussed in Chs 4 and 18.

124 Centrelink (2008) <www.centrelink.gov.au> at 21 April 2008.

125 See, eg, *Privacy (Private Sector) Regulations 2001* (Cth) reg 9.

30.95 In its submission to IP 31, the OPC suggested that the 'Identifiers' principle should regulate the adoption, use and disclosure by organisations of identifiers issued by state and territory agencies. The OPC noted that this would be in line with guidelines that it issued prior to the introduction of the NPPs.[126] The OPC also submitted that regulating the handling of all identifiers by organisations 'may be an appropriate response to emerging challenges posed by the risks of identity theft and fraud'.[127]

30.96 In DP 72, the ALRC proposed that the 'Identifiers' principle should regulate the use by agencies and organisations of identifiers assigned by state and territory agencies.[128]

Submissions and consultations

30.97 This proposal was generally supported by stakeholders.[129] In particular, privacy commissioners noted that individuals make inquiries about the collection of driver's licence numbers by organisations.[130] On the other hand, one organisation was concerned that the proposed regulation would require significant amendment to its systems.[131]

30.98 The AGD submitted that including identifiers assigned by state and territory agencies in the definition of 'identifier' would remove an inconsistency in NPP 7, but would compound the problem of identity verification.[132] Similarly, Telstra was concerned that the proposal would prevent organisations from verifying the identity of individuals as required by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).[133]

---

126 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Office of the Privacy Commissioner, *National Principles for the Fair Handling of Personal Information* (1999); Office of the Privacy Commissioner, *Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs, Inquiry into the Privacy Amendment (Private Sector) Bill 2000*, May 2000.

127 Office of the Privacy Commissioner, *Submission PR 281*, 13 April 2007. Identity theft is discussed in Ch 12.

128 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 27–4.

129 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Confidential, *Submission PR 535*, 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; Queensland Government, *Submission PR 490*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007. Another stakeholder did not disagree: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

130 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007 and Confidential, *Submission PR 535*, 21 December 2007.

131 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

132 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

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

ALRC's view

30.99 The 'Identifiers' principle should apply to identifiers such as driver's licence numbers that are assigned by state and territory agencies and used by organisations. In the ALRC's view, the adoption, use and disclosure of these identifiers by organisations raises the same privacy concerns as those associated with other identifiers.

30.100 The ALRC notes that the 'Identifiers' principle does not regulate the situation where an identifier is merely sighted by an organisation, rather than collected for inclusion in a record and then used or disclosed by that organisation. The ALRC does not suggest that the practice of an organisation sighting an identifier contained on, for example, a driver's licence should be regulated. Further, the ALRC notes earlier in this chapter that the 'Identifiers' principle is directed towards identification (determining who an individual is), rather than verification or authentication (verifying that an individual is who or what he or she claims to be). In many situations, an organisation will need only to sight the driver's licence of an individual to verify that he or she is permitted to, for example, purchase alcohol because he or she is at least 18 years of age—the organisation will not need to identify that individual.

30.101 Finally, the ALRC notes that the recommended change would not result in the regulation of acts and practices of state and territory agencies but rather the use by organisations of identifiers allocated by state and territory agencies.

Recommendation 30–5 The 'Identifiers' principle should regulate the adoption, use and disclosure by organisations of identifiers that are assigned by state and territory agencies.

Regulation of identifiers assigned by organisations

30.102 NPP 7 does not regulate the adoption, use and disclosure by organisations of identifiers assigned by other organisations. It does define, however, an identifier as including 'a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations'.[134]

30.103 In its submission to DP 72, the AGD suggested that the ALRC's 'focus on government-issued identifiers … overlooks the significant and increasing role of private sector identifiers, such as account and membership numbers'.[135] Amendment of the 'Identifiers' principle to regulate the adoption, use or disclosure by organisations of identifiers issued by other organisations was not raised by other stakeholders.

---

134 *Privacy Act 1988* (Cth), NPP 7.

135 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

ALRC's view

30.104 The ALRC heard no concrete example of harm resulting from the use and disclosure of identifiers assigned by organisations. It is unlikely that an organisation's use or disclosure of an identifier assigned by another organisation, such as a bank account number, will lead to a de facto national identification scheme. The ALRC notes, however, that such use or disclosure may facilitate data-matching activities undertaken by organisations. In Chapter 10, the ALRC recommends that the OPC should issue guidance on data-matching that relates to organisations.[136]

Multi-purpose identifiers

30.105 This section discusses identifiers assigned to individuals by governments for use by multiple government agencies and organisations (multi-purpose identifiers). The section commences by providing an overview of concerns that have been expressed about the impact on privacy of multi-purpose identifiers. It then examines the history of identification schemes in Australia before discussing the recently abandoned access card scheme. Finally, the ALRC makes a recommendation to address the privacy concerns associated with unique multi-purpose identifiers.

Benefits and privacy concerns

30.106 Schemes involving multi-purpose identifiers can have a number of benefits. For example, they can increase administrative efficiency and enhance data accuracy.[137] The existence of multi-purpose identifiers, however, also raises a number of privacy concerns. One such concern is that the introduction of a multi-purpose identifier changes fundamentally the relationship between the individual and government.[138] In liberal democratic societies, governments are accountable to their citizens. It has been argued that the introduction of a multi-purpose identifier symbolically reverses this tradition, making citizens accountable to their governments.[139] This could then open the way for 'further extensions of government power and … further restrictions on the individual's sphere of independent action'.[140]

30.107 It also is argued that linking a multi-purpose identifier to a name limits the ability of individuals to use different names in different contexts.[141] At common law, there is nothing to prevent an individual from operating under various names, provided

---

136 Rec 10–4.

137 See, eg, Council of Europe, *The Introduction and Use of Personal Identification Numbers: The Data Protection Issues* (1991).

138 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [3.7].

139 G de Q Walker, 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal' (1986) 16 *Queensland Law Society Journal* 153, 163.

140 Ibid, 163.

141 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [3.37].

that he or she does not use different names to engage in unlawful behaviour.[142] Aliases may be used by a variety of people, such as artists, authors and intelligence operatives.[143]

30.108 Further, the introduction of multi-purpose identifiers increases the ability of the state to monitor the activities of its citizens. By recording multi-purpose identifiers during transactions, government agencies and organisations can compile substantial amounts of information about a person, including information about a person's financial circumstances, family composition, hobbies or health. This could then be used for a variety of purposes, such as to locate a person or to determine a person's interests for the purposes of direct marketing.

30.109 Different agencies or organisations could then combine the data collected about the transactions or activities of particular individuals to create a richer dataset. This process is known as data-matching.[144] The use of a multi-purpose identifier facilitates greatly the data-matching process. The ability of a government to compile dossiers of personal information about individuals could have a 'chilling effect' on the activities of citizens, who no longer have a private sphere in which to relax, experiment or engage in creative pursuits.[145]

30.110 In addition, the unintended dissemination of either the identity information required to be provided by individuals in order to receive a multi-purpose identifier, or data generated by the use of the multi-purpose identifier, can erode the privacy of the individual to whom the information relates.[146] For example, such information could be stolen by a 'hacker'; accidentally disclosed through an administrative error; or deliberately sold by those with access to it, such as employees of agencies. This can increase the risk that the individual will subsequently become the victim of identity theft.[147]

30.111 Another privacy concern relates to the quality of the data involved in an identification scheme involving multi-purpose identifiers. Errors inputting data for the purposes of the scheme, or corruption of stored data, could impact adversely on the ability of individuals to access the services for which the multi-purpose identifier is required.

---

142 Ibid, Addendum, [22].

143 R Clarke, 'Just Another Piece of Plastic for your Wallet: The "Australia Card" Scheme' (1987) 5 *Prometheus* 1, 40.

144 Chs 9 and 10 discuss data-matching in detail.

145 G de Q Walker, 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal' (1986) 16 *Queensland Law Society Journal* 153, 160–161.

146 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 14.

147 Identity theft is discussed in Ch 12.

30.112 Finally, it has been argued that identity documents have had a long history of discriminatory uses for social control.[148] One commentator has noted that slaves in the United States were required to carry identification papers to travel, Nazis used identification cards to locate Jewish people during World War II, and the slaughter of Tutsis in Rwanda was aided by the fact that their identity cards revealed their ethnicity.[149]

History of identification schemes in Australia

Identification schemes in wartime

30.113 Several identification schemes were implemented in wartime Australia. During World War I and World War II, all aliens (non-British subjects) were required to register with local government officials.[150] After registration, they were required to notify officials if they changed their address[151] and to produce their certificates of registration on demand.[152] In 1942, all residents of 16 years of age or above (other than aliens and other specified groups, such as members of the Defence Force performing continuous full-time war service) were required to register with local government officials in order to obtain an identity card.[153] They were then required to produce their identity cards if requested to do so by specified people, such as constables on duty.[154]

The Australia Card

30.114 In September 1985, the Australian Government announced its intention to develop a national identification scheme—the 'Australia Card' scheme[155]—to combat tax fraud, social security fraud and illegal immigration.[156] In May 1986, a Joint Select Committee on an Australia Card delivered a report that strongly recommended against the introduction of the Australia Card. The Committee suggested a number of alternative reforms such as: the computerisation of all state and territory registries of

148 R Sobel, 'The Demeaning of Identity and Personhood in National Identification Systems' (2002) 15 *The Harvard Journal of Law and Technology* 319, 343. See also Privacy International, *Some Personal Views from Around the World on ID Cards* (1996) <www.privacyinternational.org> at 1 May 2008.

149 R Sobel, 'The Demeaning of Identity and Personhood in National Identification Systems' (2002) 15 *The Harvard Journal of Law and Technology* 319, 343–349.

150 *War Precautions (Alien Registration) Regulations 1916* (Cth) reg 5; *Aliens Registration Act 1939* (Cth) ss 8, 13(1).

151 *War Precautions (Alien Registration) Regulations 1916* (Cth); *Aliens Registration Act 1939* (Cth) ss 9–12.

152 *War Precautions (Alien Registration) Regulations 1916* (Cth) reg 12.

153 *National Security (Man Power) Regulations 1942* (Cth) reg 32.

154 Ibid regs 45, 45A.

155 P Keating (Treasurer), *Reform of the Australian Taxation System: Statement by the Treasurer The Hon Paul Keating*, 1 September 1985, 28–31.

156 R Clarke, 'Just Another Piece of Plastic for your Wallet: The "Australia Card" Scheme' (1987) 5 *Prometheus* 1, 33; Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), Addendum, [28].

births, deaths and marriages;[157] and the introduction of an upgraded, high-integrity tax file number scheme.[158]

30.115 In October 1986, the Australia Card Bill 1986 (Cth) was introduced into Parliament. On two occasions the Australia Card Bill was passed by the House of Representatives[159] only to be rejected by the Senate.[160] Under s 57 of the *Australian Constitution* this became a potential trigger for a double dissolution election. Accordingly, in May 1987, the Australian Government announced Australia's sixth double dissolution election.[161] On 11 July 1987, the Australian Labor Party was returned to office and the Australia Card Bill was reintroduced into Parliament for a third time. The Bill was ultimately laid aside after Opposition senators indicated that they would disallow regulations that were required to bring crucial clauses of the Bill into effect.[162]

Other proposed identification schemes

30.116 After the bombings in London in July 2005, the then Prime Minister of Australia stated that the introduction of a national identification scheme was an issue that should be 'back on the table'.[163] The introduction of such a scheme was discussed on a number of occasions during 2005 and early 2006.[164] On 26 April 2006, however, it was announced that the Australian Government did not intend to proceed with the introduction of a compulsory national identity card. It did intend, however, to introduce a new card that would be required to access health and welfare benefits (the access card).[165]

The access card

Overview

30.117 The access card scheme was intended to enable consumers to access all health and social services with one card; access emergency relief payments through automatic

---

157 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), rec 2(a).

158 Ibid, rec 12(a)–(d).

159 On 14 November 1986 and 25 March 1987: See R Jordan, *E-brief: Identity Cards* (2006) Parliament of Australia—Parliamentary Library <www.aph.gov.au> at 1 May 2008.

160 On 10 December 1986 and 2 April 1987: See Ibid.

161 R Clarke, 'The Australia Card: Postscript' (1988) 18 *Computers & Society* 10, 10; G Greenleaf, 'Lessons from the Australia Card—Deux ex Machina?' (1988) 3(6) *Computer Law and Security Report* 6, 6.

162 G Greenleaf, 'Lessons from the Australia Card—Deux ex Machina?' (1988) 3(6) *Computer Law and Security Report* 6, 6.

163 J Howard (Prime Minister), *Doorstop Interview*, 15 July 2005.

164 See, eg, C Keller, 'Identity Card Way to Prevent Rau Case: Vanstone', *The Advertiser* (Adelaide), 25 January 2006, 17; 'PM's Open Mind on ID Card', *The Australian* (Sydney), 25 January 2006, 2; M Priest, 'Ruddock to Push National Identity Card', *Australian Financial Review* (Sydney), 16 January 2006, 1.

165 J Howard (Prime Minister), P Ruddock (Attorney-General) and J Hockey (Minister for Human Services), *Joint Press Conference*, 26 April 2006.

teller machines and through Electronic Funds Transfer at Point of Sale (EFTPOS);[166] and reduce fraud in relation to Australian Government benefits.[167]

30.118 The access card would have replaced up to 17 existing health care and social services cards and vouchers.[168] It would have displayed the cardholder's name and photograph on its front, and the cardholder's signature and card number on its back.[169] Other personal information, such as the cardholder's photograph, date of birth, concession status, and details of the cardholder's children or dependants would have been stored on a microchip embedded in the card.[170] Information on the card and the chip would have been stored on a database that would have been maintained separately from existing agency databases.[171]

30.119 The Human Services (Enhanced Service Delivery) Bill 2007 (Cth), was introduced into the House of Representatives on 7 February 2007. The Bill provided a framework for the introduction of the proposed access card scheme[172] and stated that the purpose of the scheme was to improve the delivery of Commonwealth services and reduce fraud, particularly in relation to identity theft.[173] Later legislation was intended to provide detail on aspects of the scheme such as information protection, uses of the card, and review and appeal processes.[174]

30.120 On 8 February 2007, the provisions of the Bill were referred for inquiry to the Senate Standing Committee on Finance and Public Administration (the Committee).[175] The Committee released its report on 15 March 2007.[176] The Committee endorsed the goals of the proposed access card scheme[177] but noted that a number of privacy concerns that related to the architecture of the scheme were not dealt with by the Bill.[178]

---

166 Australian Government Office of Access Card, *Fact Sheet—Emergency Payments* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/emergency-payments.pdf> at 31 July 2007.

167 Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 7.

168 The health care and social services cards and vouchers that were to be replaced by the access card included the PBS Entitlement Card, PBS Safety Net Concession Card, Pensioner Concession Card, Centrelink Health Care Card (including a Low Income Health Care Card and a Foster Child Health Care Card), Reciprocal Health Care Card, Commonwealth Seniors Health Card, Cleft Lip and Palate Card, DVA Gold, White and Orange Cards, War Widow/Widower Transport Card, Medicare Card, and other cards or vouchers prescribed by the regulations: Ibid cl 4.

169 Ibid cls 70–71.

170 Ibid cls 73–74.

171 Ibid cl 35; Australian Government Office of Access Card, *Fact Sheet—No Mega Database* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/no-mega-database.pdf> at 31 July 2007.

172 Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 3.

173 Ibid cls 6, 7.

174 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 February 2007, 3 (M Brough—Minister for Families Community Services and Indigenous Affairs), 3.

175 Parliament of Australia—Senate Standing Committee on Finance and Public Administration, *Human Services (Enhanced Service Delivery) Bill 2007 [Provisions]* (2007).

176 Ibid.

177 Ibid, 11.

178 Ibid, 11. In addition, an Access Card Consumer and Privacy Taskforce was established to provide advice to the Australian Government on a range of matters relating to the structure and operation of the Access

30.121 At the time the federal election was called in October 2007, the Australian Government was conducting consultations on a revised exposure draft of access card legislation.[179] Shortly after winning the federal election in November 2007, the Australian Labor Party announced it would not proceed with the access card scheme.[180]

Privacy and the access card scheme

30.122 A number of concerns were expressed about the potential impact of the access card scheme on privacy. Some argued that the access card scheme was the same as the failed Australia Card scheme.[181] Other commentators were concerned about: profiling of individuals through the use of access card numbers;[182] accessing of the database for illegitimate purposes; [183] and the possibility for 'function creep'[184] if new legislation required or authorised the use or disclosure of personal information collected for the access card scheme, or new uses for the access card.[185]

Regulation of multi-purpose identifiers

30.123 In light of the above, in IP 31 the ALRC asked what role the *Privacy Act* should play in the regulation of multi-purpose identifiers.[186]

30.124 In DP 72, the ALRC expressed the view that the policy intent of NPP 7 remains relevant for Australian Government identification schemes, such as the proposed access card scheme. The ALRC noted that multi-purpose identifiers such as

---

Card scheme, including community views on the scheme and the impact of the scheme on privacy. The Taskforce published several consultation papers and reports on the access card scheme: see, eg, Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 1: The Australian Government Health and Social Services Access Card* (2006); Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 2: Voluntary Medical and Emergency Information* (2007); Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 3: Registration* (2007); Acccess Card Consumer and Privacy Taskforce, *Report Number 2: Voluntary Medical and Emergency Information on the Access Card* (2007); Access Card Consumer and Privacy Taskforce, *Report Number 3: The Access Card Review and Appeals System* (2007); Access Card Consumer and Privacy Taskforce, *Report Number 5: Registration* (2007).

179 Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth).

180 Commonwealth, *Parliamentary Debates*, Senate, 13 February 2008, 47 (J Ludwig—Minister for Human Services); K Dearne, 'Labor Swift to Dump Access Card', *The Australian* (online), 7 December 2007, <www.australianit.news.com.au>.

181 See, eg,G Greenleaf, 'Australia's Proposed ID Card: Still Quacking Like a Duck' (2007) 23 *Computer Law & Security Report* 156.

182 See, eg, Australian Privacy Foundation, *Why Every Australian Should Oppose the 'Access Card': The Arguments Against a National ID Card System* (2006).

183 See, eg, Ibid; 'Centrelink Scandal Highlights Smartcard Fears', *The Epoch Times* (online), 25 August 2006, <www.theepochtimes.com>.

184 Function creep occurs when personal information or a system is used in a manner that was unintended at the time the information was collected or the system devised: Office of the Privacy Commissioner, *An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies*, Consultation Draft (2004), [3].

185 See, eg, M Franklin, 'MP Warns of Access Card Misuse', *The Courier-Mail* (Brisbane), 18 July 2006, 4; A Stafford, 'Access Card Could Link to Surveillance', *The Age* (Melbourne), 5 June 2006, 9.

186 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 12–3.

the proposed access card number would likely fall within the definition of 'identifier' in the 'Identifiers' principle. Any exceptions to the 'Identifiers' principle should be set out clearly in legislation establishing such schemes. To this end, the ALRC proposed that before introducing a multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should consider the need for a privacy impact assessment (PIA).[187]

Submissions and consultations

30.125 Several agencies expressed support for the practice of conducting a PIA before introducing a multi-purpose identifier.[188] The Department of Human Services supported the ALRC's proposal on the basis that it afforded flexibility to the Australian Government by not mandating the requirement for a PIA but allowing the Government to consider whether there was a need for a PIA.[189]

30.126 On the other hand, a number of stakeholders submitted that the ALRC's proposal would not provide individuals with sufficient privacy protection.[190] The OVPC submitted that mandatory PIAs should be required in the context of multi-purpose identifiers.[191] The OPC supported mandatory PIAs in cases where significant privacy risks are anticipated, and submitted that multi-purpose identifiers often create such risks.[192]

30.127 The Cyberspace Law and Policy Centre submitted that, for the regulation of multi-purpose identifiers,

> [a]ny variations from the application of any of the principles should be defined by specific legislative provisions stating exceptions or variations, and not left to inference from the existence of a different set of principles. Such an approach will (i) ensure that variations are obvious; (ii) facilitate a consistent body of law emerging on both the core principles and the exceptions.[193]

ALRC's view

30.128 The ALRC has not recommended that the 'Identifiers' principle apply to agencies. Multi-purpose identifiers, however, pose significant privacy risks.

---

187 PIAs are discussed in Ch 47.

188 Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

189 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

190 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; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

191 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

193 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

Accordingly, such identifiers should be established by legislative schemes that set out clearly the exceptions to the 'Identifiers' principle. The 'Identifiers' principle would regulate the adoption, use and disclosure by organisations of multi-purpose identifiers where this is not addressed by specific legislative regimes establishing such identifiers.

30.129 The potential privacy risks of multi-purpose identifiers are always so significant that the Australian Government, in consultation with the OPC, should be required to conduct a PIA before the introduction by agencies of any multi-purpose identifier. This proactive approach encourages agencies to incorporate privacy and security safeguards into the design of multi-purpose identifiers.

Recommendation 30–6 Before the introduction by an agency of any multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should conduct a Privacy Impact Assessment.

Regulation of Tax File Numbers

Background to the enhanced TFN scheme

30.130 In May 1988, following the demise of the Australia Card scheme, the then Treasurer, the Hon Paul Keating MP, announced that the Australian Government intended to introduce an enhanced TFN scheme.[194] In 1988, legislation establishing such a scheme was passed.[195]

30.131 Before 1988, TFNs were simply numbers used by the ATO to match taxpayers' returns to the ATO's computer records.[196] No evidence of identity was required before a TFN was allocated to a taxpayer and there was no widespread use of TFNs by employers or employees.[197] The enhanced TFN scheme was designed to reduce tax evasion by improving the ATO's ability to match information received from certain sources, such as financial institutions and employers, to individual tax returns.[198]

194 P Keating (Treasurer), *Reform of the Australian Taxation System: Statement by the Treasurer The Hon Paul Keating*, 1 September 1985.
195 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).
196 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [4.8].
197 Ibid, [4.8].
198 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 September 1988, 858 (P Keating—Treasurer).

30.132 At the time the TFN scheme was introduced there were concerns that it would become a 'de facto national identification scheme',[199] and the legislation introducing the scheme contained provisions to safeguard against this. For example, it contained a provision making it an offence to require or request a TFN (including the TFN of entities other than natural persons) in unauthorised circumstances.[200] In addition, the *Privacy Act*, which was passed around the same time as the legislation introducing the enhanced TFN scheme, contained provisions designed to protect the privacy of individuals under the new TFN scheme.

30.133 The TFN scheme has been expanded since it was introduced in 1988. For example, since 1991 individuals have been required to provide their TFNs in order to obtain any federal income support.[201] One commentator has stated that function creep in the TFN scheme demonstrates 'how privacy promises made in law can be lost over a very short period of time'.[202]

Overview of TFN regulation

Legislation

30.134 The handling of TFNs is regulated under various federal Acts. For example, Part VA of the *Income Tax Assessment Act 1936* (Cth) includes provisions allowing the Commissioner of Taxation to supply correct TFNs to financial institutions if a person has quoted an incorrect TFN. The *Taxation Administration Act 1953* (Cth) prohibits requirements that TFNs are to be quoted or recorded.[203] Other pieces of legislation regulating TFNs include the *Superannuation Industry (Supervision) Act 1993* (Cth), *Income Tax (Deferred Interest Securities) (Tax File Number Withholding Tax) Act 1991* (Cth), and the *Social Security Act 1991* (Cth).

30.135 The *Data-matching Program (Assistance and Tax) Act 1990* (Cth), and guidelines issued under that Act,[204] regulate data-matching using TFNs. Data-matching involves bringing together data from different sources and comparing them. Much of the data-matching done by Australian Government agencies subject to the *Privacy Act* is to identify people for further action or investigation for overpayment or fraud.[205]

---

199 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Feasibility of a National ID Scheme; The Tax File Number* (1988), Ch 10.

200 *Taxation Administration Act 1953* (Cth) s 8WA. Section 8WB of the *Taxation Administration Act 1953* (Cth) makes it an offence to record, use or disclose a person's TFN in unauthorised circumstances.

201 Office of the Federal Privacy Commissioner, *Submission to the House of Representatives Standing Committee on Economics, Finance and Public Administration Review of the ANAO Audit Report No. 37 1998–99 on the Management of Tax File Numbers*, 1 November 1999, Attachment E.

202 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 13.

203 Subject to exceptions: *Taxation Administration Act 1953* (Cth) pt III div 2 subdiv BA.

204 Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997). These Guidelines replaced the Guidelines originally set down in sch 2 to the *Privacy Act 1988* (Cth).

205 Office of the Privacy Commissioner, *Data-Matching* <www.privacy.gov.au/act/datamatching> at 1 May 2008. Data-matching is also discussed in Chs 9 and 10.

Tax File Number Guidelines

30.136 Section 17 of the *Privacy Act* enables the Privacy Commissioner to issue legally binding guidelines concerning the collection, storage, use and security of 'tax file number information'.[206] 'Tax file number information' is defined as 'information … that records the tax file number of a person in a manner connecting it with the person's identity'.[207] The Privacy Commissioner's guidelines are binding on all 'file number recipients'[208]—namely, people who are 'in possession or control of a record that contains tax file number information'.[209]

30.137 The Privacy Commissioner published *Tax File Number Guidelines* (TFN Guidelines) in 1992.[210] These Guidelines provide that the TFN scheme is not to be used as a national identification scheme.[211] In no situation is it mandatory for an individual to disclose his or her TFN, although non-disclosure in certain situations may have adverse financial consequences. For example, if an individual chooses not to quote his or her TFN when commencing employment, he or she will be taxed at the maximum applicable tax rate.[212] TFNs can be collected only by certain persons and organisations[213] and must not be used to establish or confirm an individual's identity for a purpose not authorised by taxation, assistance agency or superannuation law.[214] In addition, TFNs are not to be used to match personal information about an individual except as authorised by taxation, assistance agency or superannuation law.[215]

Fragmentation of regulation

30.138 In IP 31, the ALRC asked whether federal legislation relating to the handling of TFNs and data-matching should be consolidated in the *Privacy Act*.[216] In DP 72, the ALRC expressed the view that there was no compelling reason to consolidate the federal legislation relating to the handling of TFNs and data-matching of TFNs. The

206 Interim guidelines set out in sch 2 of the *Privacy Act* applied until the Privacy Commissioner's guidelines issued under s 17 took effect: *Privacy Act 1988* (Cth) s 17(4).
207 Ibid s 6.
208 Ibid s 18.
209 Ibid s 11.
210 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
211 Ibid, 1.1.
212 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 12.
213 The Privacy Commissioner and the former Insurance and Superannuation Commissioner (now the Australian Prudential Regulation Authority (APRA)), have complied a list of 'Classes of Lawful Tax File Number Recipients': see Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
214 Ibid, [2.1], [5.1].
215 Ibid, [2.3].
216 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(g).

ALRC agreed with the OPC that the consolidation in the *Privacy Acts* of the various TFN provisions and offences would not be a 'comfortable fit'.[217]

30.139 This issue was not the subject of submissions and consultations in response to DP 72. In the ALRC's view, the current regulation of TFNs is appropriate.

Effectiveness of current regulation

30.140 In IP 31, the ALRC asked whether the schemes that regulate TFNs remain effective.[218] The Australian Privacy Foundation submitted that there had been developments in data-matching and identity management technology since the introduction of the TFN Guidelines in 1992. There had also been function creep in the TFN scheme.[219] Some stakeholders expressed concern about the burden of compliance associated with TFN regulation.[220]

30.141 In DP 72, the ALRC proposed that the TFN Guidelines should be subject to a review by the OPC. The ALRC agreed with the OPC that such a review would 'be consistent with good regulatory practice, which holds that regulatory instruments be reviewed at intervals of no more than 10 years'.[221]

Submissions and consultations

30.142 Support for this proposal was widespread.[222] For example, the Investment and Financial Services Association submitted that such a review was necessary because of 'substantial changes in technology and the processes which industry members use when managing documents containing TFNs'.[223]

30.143 The OPC suggested that the proposed review would provide an opportunity to consult with stakeholders on ways to improve the guidelines.[224] Several stakeholders expressed their willingness to be involved in the review process.[225]

---

217 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

218 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 12–2.

219 See, eg, Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

220 Mortgage and Finance Association of Australia, *Submission PR 231*, 9 March 2007; Link Market Service, *Submission PR 2*, 24 February 2006.

221 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

222 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; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

223 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

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

225 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

ALRC's view

30.144 The TFN Guidelines should be subject to a review by the OPC. Such a review could be conducted in consultation with the ATO and other relevant stakeholders, and could consider any relevant developments in technology since the introduction of the TFN Guidelines, and the regulatory burden imposed by current TFN regulation. Any consideration of the compliance burden must be balanced against the policy reasons underpinning the privacy protections afforded to TFNs.

30.145 Further, as discussed in Chapter 47, the TFN Guidelines should be renamed the TFN Rules to reflect that the guidelines are binding and that a breach constitutes an interference with privacy under s 13 of the *Privacy Act*.[226]

Recommendation 30–7 The Office of the Privacy Commissioner, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the Tax File Number Guidelines issued under s 17 of the *Privacy Act*.

Summary of 'Identifiers' principle

30.146 The tenth principle in the model UPPs should be called 'Identifiers'. It may be summarised as follows.

UPP 10. Identifiers (only applicable to organisations)

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency;

(b) an agent of an agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

226 *Privacy Act 1988* (Cth) s 13(b). See Rec 47–2.

10.2 Where an identifier has been 'assigned' within the meaning of UPP 10.1 an organisation must not use or disclose the identifier unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier;

(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure; or

(c) the identifier is genetic information and the use or disclosure would be permitted by the new *Privacy (Health Information) Regulations*.

10.3 UPP 10.1 and 10.2 do not apply to the adoption, use or disclosure by a prescribed organisation of a prescribed identifier in prescribed circumstances, set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

10.4 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

(a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or

(b) is determined to be an identifier by the Privacy Commissioner.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

Note: A determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003* (Cth).

31. Cross-border Data Flows

Contents

Introduction

31.1 Cross-border data flow refers to the movement of personal information (or data) across national borders.[1] While the focus of the *Privacy Act* 1988 (Cth) was originally

1 See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Part IV, Section B. See also Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 1 (the OECD uses the terminology 'transborder data flow'). In Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), the 'Cross-border Data Flows' principle was referred to as the 'Transborder Data Flows' principle, picking up on the terminology used currently in NPP 9. The ALRC has changed the name of this

on personal information collected and handled within Australia, the increasing ease with which information can be transferred between countries has forced jurisdictions to recognise that efforts to protect personal information should be harmonised.[2]

> Modern business is increasingly borderless. The communications revolution and the reduction in international trade barriers has allowed business to globalise and for regions to specialise. The call centre answers the phone in India, the product is designed in Europe, made in China and it is all managed from the US. But these business units must share their information; information about employees, customers and suppliers.[3]

31.2 Overseas business processing centres are increasingly handling customer data in such sensitive areas as processing credit card applications and bills, mortgage applications, insurance claims and help desk services.[4] One of the current leaders in this sphere is India which controls, according to some estimates, '44% of the global outsourcing market of software and back-office services'.[5] India's total revenue due to IT and business process outsourcing is expected to grow to $60 billion by 2010.[6] Steven Robertson notes that China's outsourcing industry is beginning to 'rival the outsourcing powerhouse, India'.[7] Some commentators have pointed out that 'currently no data privacy protection legislation of any kind exists in India'.[8] Similarly, at present, China has 'no consolidated national data protection legislation'.[9]

31.3 A number of incidents have highlighted how personal information may be at risk from cross-border data flows.[10] For example, in 2005, undercover reporters from the Australian Broadcasting Corporation 'were allegedly offered for sale personal data of 1,000 Australians for around US$10 per person'. The data included names, birth certificate details, drivers licence details and ATM card numbers.[11] It is important for

---

principle, however, to make it consistent with terminology more commonly used, such as in the APEC Privacy Framework: Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [44]–[46].

2 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), vii.

3 K Sainty and A Ailwood, 'Implications of Transborder Data Flow for Global Business' (2004–2005) 1 *Privacy Law Bulletin* 101, 101. See also N Saravade and P Kumaraguru, 'Data Security Council of India—A Self-Regulatory Initiative in Data Security and Privacy Protection' (2007) 7(11) *IAPP* 1, 1.

4 B Cruchfield George and D Roach Gaut, 'Offshore Outsourcing to India by EU and US Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing' (2006) 6 *University of California Business Law Journal* 13, 13.

5 Ibid.

6 N Saravade and P Kumaraguru, 'Data Security Council of India—A Self-Regulatory Initiative in Data Security and Privacy Protection' (2007) 7(11) *IAPP* 1, 1.

7 S Robertson, 'Offshore Business Processing in China Brings Privacy Concerns' (2008) 10 *Internet Law Bulletin* 118, 118.

8 B Cruchfield George and D Roach Gaut, 'Offshore Outsourcing to India by EU and US Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing' (2006) 6 *University of California Business Law Journal* 13, 13.

9 S Robertson, 'Offshore Business Processing in China Brings Privacy Concerns' (2008) 10 *Internet Law Bulletin* 118, 118.

10 D Giles and A Chotar, 'Offshoring Personal Information—The Devil in the Detail' (2006) 3(6&7) *Privacy Law Bulletin* 73, 73.

11 Ibid, 73–74.

Australians to feel confident that if their personal information is transferred outside Australia, it will be protected to the same standard that they enjoy in Australia.

31.4 Cross-border transfers of personal information have been, and continue to be, the source of significant community concern. For example, in a survey commissioned by the Office of the Privacy Commissioner (OPC), the majority of respondent Australians (90%) were 'concerned' about businesses sending their personal information overseas—of those, 63% were 'very concerned'.[12] Such concerns were also reflected in the National Privacy Phone-In conducted by the ALRC, in which a number of respondents expressed concern about Australian companies sending their personal information offshore, particularly to overseas call centres.

> If I deal with a company in Australia, I most certainly do not want that company passing my details overseas, where laws about privacy are even weaker. I also have a right to know when paying online whether my payment details are being sent overseas, as I view this as a huge security risk.[13]

31.5 Another stakeholder stated:

> In today's truly globalised world, cross-border data flows are an everyday fact of commercial public and private life. The challenge therefore becomes how to maintain a consistent security and privacy framework around the treatment of that information across legal and jurisdictional borders and geographies.[14]

31.6 One commentator**,** Associate Professor Dan Svantesson, noted that without adequate protection against cross-border data flows, 'privacy regulation would arguably be pointless as personal information simply would be transferred to other jurisdictions without privacy protection'.[15]

31.7 Economic development is dependent on globalisation of information and electronic commerce. In the 1970s and 1980s, international bodies developed the first instruments to harmonise laws within economic communities and improve trade relationships. The 1980 Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) was one of the first international instruments that attempted to address this issue.

31.8 The OECD Guidelines provide that, in developing laws and policies to protect privacy and individual liberties, member countries should not enact laws that

---

12 Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), 36.

13 *National Privacy Phone-In* June 2006, Comment No 433. See also Unisys, *Submission PR 569*, 12 February 2008; B Laing, *Submission PR 339*, 12 November 2007; and D Giles and A Chotar, 'Offshoring Personal Information—The Devil in the Detail' (2006) 3(6&7) *Privacy Law Bulletin* 73, 74, citing research conducted by Blair Ingenuity.

14 Unisys, *Submission PR 569*, 12 February 2008.

15 D Svantesson, 'Protecting Privacy on the "Borderless" Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168, 179.

unnecessarily create obstacles to cross-border flows of personal data.[16] The privacy principles in the OECD Guidelines are the foundation for the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) set out in the *Privacy Act*. NPP 9 governs cross-border data flow out of Australia.[17]

31.9 More recent examples of these instruments are the privacy principles adopted by the European Union (EU) under the 1995 *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*[18] (EU Directive) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[19] The Asia-Pacific Privacy Charter Council, a regional non-government expert group, is also developing independent privacy standards for privacy protection in the Asia-Pacific region.[20] Australia's ability to meet the expectations of privacy protection demanded by the international community is important to ensure that Australian businesses are not disadvantaged in an international market.

31.10 In this chapter, the ALRC examines international frameworks for privacy protection, in particular, the EU Directive, the APEC Privacy Framework and the Asia-Pacific Privacy Charter. It then considers the regulation of cross-border data flows under the *Privacy Act* via the extraterritorial operation of the Act, and the restrictions in NPP 9 on the transfer of personal information to countries with differing privacy regimes. The content of the 'Cross-border Data Flows' principle in the model Unified Privacy Principles (UPPs) is then considered, and its application to agencies is discussed. Finally, the application of the 'Cross-border Data Flows' principle to related bodies corporate, the role of the Privacy Commissioner, notification requirements and the need for OPC guidance are addressed.

International privacy protection

31.11 In order to ensure that Australian organisations are not disadvantaged in the international market, Australia must be able to meet the international community's expectations of privacy protection while not impeding the free flow of information across borders. In this section, international models of data protection are outlined.

---

16 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 18.

17 The IPPs and OECD Guidelines do not contain a comparable cross-border data principle to NPP 9. The transfer of personal information outside Australia by agencies is discussed below.

18 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

19 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

20 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 5 May 2008. These instruments are discussed later in the chapter.

European Union Data Protection Directive

31.12 The EU Directive seeks to protect the privacy of individuals within the EU when information about them is transferred to countries outside the EU.[21] If the European Commission determines that a country does not provide 'adequate' data protection standards, this will lead to restrictions on the transfer of information to that jurisdiction.[22]

31.13 Article 25(1) of the EU Directive provides:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

31.14 Article 25(4) provides:

> Where the Commission finds … that a country does not ensure an adequate level of protection … Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

31.15 Article 26 provides an exception to art 25, permitting transfers in certain circumstances to a third country, even where the third country has not ensured an adequate level of protection. The art 26 exception applies where:

- there is unambiguous consent from the data subject;
- the transfer is necessary for the performance, implementation or conclusion of certain contractual transactions;
- the transfer is in the public interest or the vital interests of the data subject; or
- the transfer is made from a public register.

31.16 Under art 26(2), a member state may also authorise transfers of personal data where a contract contains adequate safeguards protecting the 'privacy and fundamental rights and freedoms of individuals, and as regards the exercise of corresponding rights'.[23]

---

21 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

22 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 9.

23 See discussion of the use of contracts for compliance with the EU Directive below. See also A Hughes, 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)' (2001) 24 *University of New South Wales Law Journal* 270.

31.17 The decision about the adequacy of third party regimes is made by the Article 29 Data Protection Working Party of the European Commission (Working Party), which is comprised of representatives of supervisory authorities in EU member states and a representative of the European Commission. Those countries that have been declared 'adequate' are: Canada, Switzerland, Argentina, Guernsey and the Isle of Man. The US Department of Commerce's Safe Harbour Privacy Principles and the 'transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection' also have been given adequacy status.[24]

31.18 The Working Party has noted that adequate protection does not necessarily mean equivalent protection, and that it is not necessary for third countries to adopt a single model of privacy protection. It also has stated that there may be adequate protection despite certain weaknesses in a particular system 'provided, of course, that such a system can be assessed as adequate overall—for example, because of compensating strengths in other areas'.[25]

31.19 If a third country is deemed not to have adequate protection, member states must take action to prevent any transfer of personal data to the country in question. This 'mandated approach' is stronger than that set out in the OECD Guidelines.[26]

31.20 Professors Colin Bennett and Charles Raab note that the implementation of arts 25 and 26 poses problems for businesses that rely on cross-border flows of personal data. This has major implications for credit-granting and financial institutions, hotel and airline reservations systems, the direct marketing sector, life and property insurance, the pharmaceutical industry, and for any online company that markets its products and services internationally.[27]

Adequacy of the Privacy Act

31.21 One of the main drivers behind the *Privacy Amendment (Private Sector) Act 2000* (Cth) was to facilitate trade with European countries by having the *Privacy Act* deemed adequate for the purposes of the EU Directive.[28] In March 2001, however, the Working Party released an opinion expressing concern that some sectors and activities are excluded from the protection of the *Privacy Act*, including small businesses and employee records.[29] The Working Party found that, without further safeguards, the

---

24 See European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries* (2008) <ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm> at 29 April 2008. See also *Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS)*, 23 July 2007.

25 Text on Non-Discrimination adopted by the Article 31 Committee (31 May 2000), cited in D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 935.

26 C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), 99.

27 Ibid, 99.

28 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 11–12.

29 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 3.

Australian standards could not be deemed equivalent to the EU Directive. The Working Party also expressed concern about Australia's regulation of sensitive information within the *Privacy Act* and the lack of correction rights for EU citizens under the Act.[30]

31.22 Further amendments were made to the *Privacy Act* in April 2004 as part of the process of moving towards EU adequacy.[31] Those amendments:

- clarified that the protection offered by NPP 9 applies equally to the personal information of Australians and non-Australians;
- removed nationality and residency limitations on the power of the Privacy Commissioner to investigate complaints regarding the correction of personal information; and
- gave businesses and industries more flexibility in developing privacy codes that cover otherwise exempt acts.[32]

31.23 The OPC review of the private sector provisions of the *Privacy Act* (OPC Review) noted that there are ongoing discussions with the European Commission regarding the small business and employee records exemptions from the *Privacy Act*.[33] In evidence to the Senate Committee privacy inquiry, the Australian Government Attorney-General's Department noted that the small business exemption was of concern to the European Commission and that it is probably the key outstanding issue between the EU and Australia.[34] There is no equivalent in the EU Directive to the *Privacy Act* exemption for small businesses. The Senate Committee privacy inquiry questioned the need to retain the small business exemption, in part because it is preventing recognition of Australian privacy laws under the EU Directive.[35]

31.24 In evidence to the Senate Committee privacy inquiry, the Law Institute of Victoria stated:

---

30 European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (2000), 7.

31 *Privacy Amendment Act 2004* (Cth).

32 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

33 Ibid, 74.

34 Commonwealth of Australia, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 63 (C Minihan). This was confirmed more recently in a consultation with the Chair of the Article 29 Working Party: P Schaar, *Consultation OSC 1*, London, 1 November 2006. The small business exemption is discussed further in Ch 39.

35 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32]–[7.34], rec 12.

> If we do not comply with the EU directive, Australian businesses are going to be impacted in terms of the extent to which they can work offshore and deal with other jurisdictions.[36]

31.25 This view was not shared by all stakeholders making submissions to the Senate Committee privacy inquiry. For example, the Australian Direct Marketing Association (ADMA) submitted that organisations had not been hindered in their ability to conduct business with EU business partners. Similarly, the OPC stated that, in practice, businesses simply included the relevant privacy standards in contracts.[37]

31.26 The OPC Review suggested that the fact that Australian privacy law has not been recognised as adequate by the EU has not inhibited trade. It stated that

> only a very small proportion of the submissions received from stakeholders and few of the comments made in consultation meetings indicate that the failure to achieve EU adequacy has impaired business and trade with European organisations.[38]

31.27 Nevertheless, the Senate Committee privacy inquiry also considered it desirable for Australia's privacy laws to gain formal recognition as being adequate. The Senate Committee recommended that:

> the review by the Australian Law Reform Commission, as proposed at recommendations 1 and 2, examine measures that could be taken to assist recognition of Australia's privacy laws under the European Union Data Protection Directive.[39]

31.28 The EU and Australia are engaged in ongoing negotiations on the issue of the adequacy of Australia's privacy regime for the purpose of the EU Directive.

The use of contracts for compliance with the EU Directive

31.29 Alongside legislation and self-regulatory arrangements, contracts have been recognised as a mechanism for enhancing privacy protection.[40] Article 26(2) of the EU Directive explicitly recognises that contracts may be one method of ensuring that personal data transferred from one country to another receive 'adequate protection'. A contract that would meet these criteria would have to bind the organisation receiving

---

36 Ibid, [4.127].

37 Ibid, [4.130]. See also A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

38 The OPC concluded, however, that although there was no evidence of a push from business for the EU's recognition of adequacy, there may be long term benefits for Australia to continue to work towards this aim. The OPC also supported continuing work within APEC to implement the APEC Privacy Framework (discussed below): Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 75.

39 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 16.

40 Organisation for Economic Co-operation and Development, *Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks* (2000), 7.

the data to meet the EU standards of information practices, such as the right to notice, consent, access and legal remedies.[41]

31.30 The OECD has identified the following as core elements of privacy protection that should be reflected in contractual provisions:

- substantive rules based on the principles in the OECD Guidelines, either by inclusion of the substantive rules in the contract or by reference to relevant laws, principles or guidelines;
- a means of ensuring accountability and verifying that the parties are complying with their privacy obligations;
- a complaints and investigations process, in the event that there is a breach of the privacy obligations; and
- a dispute resolution mechanism for affected parties.[42]

Is 'adequacy' necessary or desirable?

31.31 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether adequacy of the *Privacy Act* under the EU Directive is necessary for the effective conduct of business with EU members, and desirable for the effective protection of personal information transferred into and out of Australia.[43] The consensus view of stakeholders was that, while a failure to achieve adequacy under the EU Directive was not preventing organisations from carrying out business internationally, an adequacy rating would help streamline trade between Australian businesses and Europe.[44] One stakeholder raised the important symbolic significance of achieving adequacy for the purposes of the EU Directive.[45] While adequacy is desirable, it was noted that, even in EU jurisdictions, privacy protection may not always be implemented satisfactorily.[46] In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC did not make a proposal in relation to the EU Directive specifically, but indicated that a number of its proposals in particular areas may assist in an EU adequacy finding.[47]

---

41 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), 361.

42 Organisation for Economic Co-operation and Development, *Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks* (2000), 13.

43 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–5. See also [13.72].

44 Stakeholder comments were canvassed in detail in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.143]–[28.147].

45 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

46 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.150].

ALRC's view

31.32 The ALRC has been advised that the EU Directive can create problems for organisations that conduct business in Europe. It has been noted that the registration system in Europe is expensive, and that adequacy under the EU Directive may still mean that organisations will be subject to additional requirements under the privacy laws of individual European countries. The ALRC also notes that the European Commission's *First Report on the Implementation of the Data Protection Directive* found that the EU Directive has not guaranteed consistent privacy protection across Europe.[48] Different jurisdictions have implemented the EU Directive in different ways and, as a result, unauthorised and possibly illegal transfers are being made to destinations.[49]

31.33 The ALRC makes a number of recommendations which may assist an adequacy finding under the EU Directive, including: the removal of the small business and employee records exemptions;[50] requiring an organisation to provide an individual with a means of opting out of receiving direct marketing communications under the 'Direct Marketing' principle;[51] and, in the context of cross-border data flows, the development and publication of a list of laws and binding schemes that effectively uphold principles for the fair handling of personal information that are substantially similar to the model UPPs.[52]

Asia-Pacific Economic Cooperation Privacy Framework

31.34 The APEC Privacy Framework was endorsed by APEC Ministers in November 2004. The APEC Privacy Framework contains nine privacy principles recognising 'the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region'.[53]

31.35 As with the EU Directive, the APEC Privacy Framework aims to promote electronic commerce by harmonising members' data protection laws and facilitating information flow throughout the Asia-Pacific region.[54] Unlike the EU Directive,

---

48 Commission of the European Communities, *Report from the Commission: First Report on the Implementation of the Data Protection Directive* (2003) 95/46/EC, 19. For areas of concern noted by the Article 29 Working Party, see: European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001); A Hughes, 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)' (2001) 24 *University of New South Wales Law Journal* 270, 272–275.

49 Commission of the European Communities, *Report from the Commission: First Report on the Implementation of the Data Protection Directive* (2003).

50 Recs 39–1, 40–1.

51 Recs 26–3, 26–4, 26–5.

52 Rec 31–6.

53 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Foreword.

54 Ibid, [4].

however, APEC members are not obliged to implement domestically the APEC Privacy Framework in any particular way.[55]

31.36 APEC commenced development of the APEC Privacy Framework in 2003. It is a principles-based framework, based largely on the OECD Principles. Australia played a key role in the development of the APEC Privacy Framework, leading the APEC working group in the drafting process.

31.37 The APEC principles are intended to apply to persons or organisations in both the public and private sectors who control the collection, holding, use, transfer or disclosure of personal information.[56] The principles cover: preventing harm; notice; collection limitation; use of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability.[57] The principles are intended to encourage the development of appropriate information privacy protections by members.[58]

31.38 One key area in which the APEC Privacy Framework takes a different approach to the EU Directive is in relation to cross-border data flows. Consultants to APEC, Malcolm Crompton and Peter Ford, have said:

> It is no longer accurate to describe data as 'flowing' at all … instead of point to point transfers, information is now commonly distributed among a number of data centres and is accessible globally over the Internet or over private networks.[59]

31.39 Principle 9 of the APEC Privacy Framework states that a personal information controller

> should be accountable for complying with measures that give effect to the Principles … When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.[60]

31.40 Given the vast differences between the member economies of APEC, the APEC Privacy Framework does not aspire to uniformity but strives to recognise cultural and other diversities within its membership.[61] It is intended to be 'implemented in a flexible manner that can accommodate various methods of implementation'.[62] The APEC

---

55 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.
56 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [10].
57 See Ibid, [14]–[26].
58 Ibid, Preamble.
59 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.
60 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 9.
61 Ibid, [5]–[6].
62 Ibid, [31].

Privacy Framework encourages cooperation between members on the regional enforcement of data protection norms and the development of agreements between nations for cooperative enforcement.[63] These cross-border arrangements may include mechanisms to:

- notify public authorities in other member states of investigations and assistance in investigations; and

- identify and prioritise cases for cooperation in severe cases of privacy infringement that may involve authorities in several countries.[64]

31.41 APEC members also have agreed to support the development and recognition of members' cross-border privacy rules (CBPRs) across the APEC region.[65] The APEC Privacy Framework states that:

> Member Economies should endeavour to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.[66]

31.42 The First Technical Assistance Seminar on International Implementation of the APEC Privacy Framework was held on 22–23 January 2007 in Canberra. Its focus was the development and use of CBPRs by business, and the development of a model for implementing CBPRs. The seminar concluded that a 'Choice of Approach' model supported by trustmarks would be the most appropriate model. The key feature of this model is that each economy chooses the entities and procedures that will be used within the economy to assess the compliance of an organisation's CBPRs with the APEC Privacy Framework.

31.43 Discussions at this meeting emphasised that trust marks could play a significant role in a CBPR system to assist economies in reviewing and giving recognition to organisations' CBPRs. A trustmark is a label or visual representation showing participation in a trustmark scheme in which a third party guarantees to consumers an organisation's compliance with the requirements for participation in that scheme. Trustmarks can be used to demonstrate compliance with a host of different principles, including privacy principles.[67]

31.44 The Second Technical Assistance Seminar on International Implementation of the APEC Privacy Framework was held in Cairns on 25–26 June 2007. It looked at

---

63 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.

64 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [45].

65 Ibid, [46].

66 Ibid, [48].

67 Trustmarks are discussed further below.

developing and refining aspects of the 'Choice of Approach' model by considering the cross-border cooperation arrangements between various stakeholders, which will be a necessary part of a CBPR system, and the steps economies can take to implement parts of the preferred implementation model. The development of a 'Pathfinder' (or pilot project), which would involve a number of economies participating in a trial of a CBPR system, was discussed at the seminar.

31.45 The OPC is currently leading three Data Privacy Pathfinder projects:[68]

- Project Five—to establish and maintain a directory of data protection authorities;
- Project Six—to develop template documentation (such as a Memorandum of Understanding (MOU) or letters of commitment) 'which provides for cooperative arrangements between relevant enforcement authorities';[69] and
- Project Seven—to develop a template for a cross-border complaint-handling form.[70]

31.46 Senator the Hon John Faulkner, Cabinet Secretary and Minister with responsibility for the *Privacy Act*, has described the aim of the Pathfinder processes as the establishment of

> a multi-lateral co-operative framework and rules, whereby a person in one country, such as Australia, can make a complaint to the privacy regulator in their own country about an alleged breach of their privacy, even though the breach affecting them may have occurred outside Australia.[71]

31.47 As noted above, Australia has been instrumental in the development of the APEC Privacy Framework. In the final report of the OPC Review, the OPC was supportive of the APEC Privacy Framework and expressed the view that:

> The initiative has the potential to accelerate the development of information privacy schemes in the APEC region and to assist in the harmonisation of standards across national jurisdictions.[72]

---

68 K Curtis, 'Information Workshop for Australian Stakeholders' (Paper presented at APEC Data Privacy Pathfinder Seminar, Sydney, 6 February 2008), 5.

69 Ibid, 5–7.

70 Ibid.

71 J Faulkner, 'Launch of Inaugural Australian Privacy Awards' (Paper presented at Privacy Connections Breakfast, Sydney, 9 April 2008), 2.

72 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 75.

31.48 Senator Faulkner also has indicated, however, that 'Australia's domestic privacy principles will not be compromised' by Australia's work in 'developing an APEC-wide cross-border privacy rules system'.[73]

Analysis of the APEC framework

31.49 Crompton and Ford note that Principle 9 of the APEC Framework is the most important difference between it and the EU Directive. In effect, the APEC Principle is saying that 'accountability should follow the data'. Once an organisation has collected personal information, it remains accountable for the data 'even if it changes hands or moves from one jurisdiction' to another. In contrast, the EU Directive focuses on border controls.[74]

31.50 There has been some criticism that the APEC Privacy Framework is too 'light touch' in its approach and does not provide sufficient privacy protection for individuals.[75] Professor Graham Greenleaf argues that the APEC Privacy Framework has a bias towards the free flow of personal information and does not recognise that there can be legitimate privacy reasons for restricting data exports.[76] The requirement of accountability, coupled with a requirement either of consent or that the discloser takes reasonable steps to protect the information, is said to be 'a very soft substitute for a Data Export Limitation principle' along the lines of that contained in the EU Directive.[77]

31.51 Greenleaf has acknowledged, however, that although the APEC Privacy Framework does not set any requirements of its own, it does not prevent its members having their own data export restriction rules. Such rules could be for domestic purposes or to meet the requirements of the EU Directive.[78]

31.52 One commentator has argued that the slow pace at which the EU's Article 29 Committee has approved the adequacy of regulatory regimes 'actually has helped reinforce the relevance of the APEC framework that increasingly is recognised as an important development'.[79]

---

73 J Faulkner, 'Launch of Inaugural Australian Privacy Awards' (Paper presented at Privacy Connections Breakfast, Sydney, 9 April 2008), 2–3.

74 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.

75 See, eg, G Greenleaf, 'APEC Privacy Framework Completed: No Threat to Privacy Standards' (2006) 11 *Privacy Law & Policy Reporter* 220; S Robertson, 'Offshore Business Processing in China Brings Privacy Concerns' (2008) 10 *Internet Law Bulletin* 118, 119.

76 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121, 122.

77 Ibid, 125.

78 G Greenleaf, 'APEC Privacy Framework Completed: No Threat to Privacy Standards' (2006) 11 *Privacy Law & Policy Reporter* 220.

79 S Kenny, 'Global Privacy Predictions for 2008' (2008) 8(1) *Privacy Advisor* 11, 12.

Asia-Pacific Privacy Charter Initiative

31.53 The Asia-Pacific Privacy Charter Council, a regional non-government expert group, has developed independent privacy standards for privacy protection in the Asia-Pacific region.[80] The Council has drafted the Asia-Pacific Privacy Charter (APP Charter) with the aim of influencing the development of privacy laws in the region in accordance with the standards set out in the Charter.[81]

31.54 The APEC Privacy Framework and the APP Charter have a number of similarities, and both reflect many of the principles contained in other international and regional agreements, such as the OECD Guidelines and the EU Directive.[82] The APP Charter, as it stands, however, is intended to be a 'maximalist' or 'high watermark' draft, reflecting all the significant privacy principles from relevant international instruments.[83]

31.55 The APEC Privacy Framework does not have a principle that explicitly limits data flows to countries without similar privacy laws. In contrast, Principle 12 of the APP Charter contains a limitation similar to that under the EU Directive. Principle 12 states that an organisation must not transfer personal information to a place outside the jurisdiction in which it is located unless:

- there is in force in that jurisdiction a law embodying principles substantially similar to the APP Charter Principles;
- it is with the consent of the person concerned; or
- the organisation has taken all reasonable steps to ensure that the personal information will be dealt with in accordance with the APP Charter Principles in that place and continues to be liable for any breaches of the Principles.

31.56 In IP 31, the ALRC asked whether the APEC Privacy Framework, or other standards, such as the APP Charter, provide an appropriate model for the protection of personal information transferred between countries.[84] A number of stakeholders supported the APEC Privacy Framework.[85] It was noted that the Framework may

---

80 Cyberspace Law and Policy Centre, 'Announcement: Asia-Pacific Privacy Charter Initiative' (Press Release, 1 May 2003). As at 29 April 2008, a second draft of the Charter had not yet been released for public comment.

81 See Ibid.

82 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 5 May 2008, 1.

83 Ibid, 1.

84 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–6.

85 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; ANZ, *Consultation PC 82*; Melbourne, 7 February 2007; Australian Compliance Institute, *Consultation PC 53*, Sydney, 17 January

function as a starting point to assist member economies that currently do not have any privacy regime to develop privacy protections for individuals' personal information.[86] Other stakeholders submitted that the APP Charter provides a more appropriate model for protecting privacy.[87]

Conclusion

31.57 The APEC Privacy Framework is a significant development in addressing regional consistency in the handling of personal information. In implementing the APEC Privacy Framework,

> the means of giving effect to the Framework may differ between Member Economies, and it may be appropriate for individual economies to determine that different APEC Privacy Principles may call for different means of implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatibility of approaches in privacy protections in the APEC region that is respectful of requirements of individual economies.[88]

31.58 The involvement of Australia in the implementation of the APEC Privacy Framework is not intended to require the lowering of any privacy protection under the *Privacy Act*.[89] It may provide, however, new ways of encouraging compliance with local and international privacy standards. The ALRC notes that the Australian Government continues to play a key role in the implementation of the APEC Privacy Framework. The ALRC has borrowed elements from both the APEC Privacy Framework and the APP Charter, as well as the NPPs and the EU Directive, in developing the 'Cross-border Data Flows' principle discussed below.[90]

Trustmarks

31.59 One feature of the APEC Privacy Framework that may have application in the Australian context is a trustmark scheme.[91] A number of countries already have adopted trustmark schemes, including privacy trustmark schemes. Some of these schemes are beginning to recognise each others' trustmarks and develop global trustmark principles.[92] Trustmark schemes vary in nature and structure. For example, in

---

2007. Stakeholder submissions were canvassed in detail in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.172]–[28.176].

86 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

87 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.176]. See also 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.

88 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [32].

89 J Faulkner, 'Launch of Inaugural Australian Privacy Awards' (Paper presented at Privacy Connections Breakfast, Sydney, 9 April 2008), 2.

90 See, eg, Rec 31–2.

91 The ALRC notes that the EU is currently considering the use of 'trust seals' in the context of privacy-enhancing technologies. See Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* (2007), 228.

92 Examples include the BBBOnline, *BBBOnline Japanese Privacy Seal* <www.bbbonline.org/privacy/jipdec.asp> at 6 May 2008; Asia Trustmark Alliance (ATA): TrustSg, *Asia Trustmark Alliance*

the United States (US), trustmark bodies are private sector organisations,[93] whereas in Singapore, the National Trust Council's trustmark 'TrustSg' is publicly supported by Singapore's Infocomm Development Authority.[94]

31.60 Trustmark bodies not only provide accreditation and allow the use of trustmarks, they also can provide advice to organisations and consumers about privacy laws, and handle privacy complaints.[95] One advantage of adopting a trustmark scheme is that it can deal with low-level privacy breaches and the provision of advice on privacy matters, leaving government regulators and law enforcement bodies to focus on serious and harmful privacy breaches.

31.61 One option would be to introduce an Australian privacy trustmark scheme. An Australian privacy trustmark scheme could approve privacy policies for the purpose of the 'Openness' principle in the model UPPs. On approval, an agency or organisation would be permitted to display a privacy trustmark. If an agency or organisation breaches an individual's privacy, a privacy trustmark body could provide an external dispute resolution scheme and could refer appropriate matters to the OPC. One enforcement option would be to prevent an agency or organisation displaying a trustmark. Once established, an Australian trustmark scheme could seek recognition by overseas trustmark schemes, and could be used to approve CBPRs for the purposes of the APEC Privacy Framework or other international privacy regimes.

31.62 In DP 72, the ALRC asked whether the use of trustmarks would be an effective method of promoting compliance with, and enforcement of, the *Privacy Act* and other international privacy regimes.[96]

Submissions and consultations

31.63 The OPC stated that it had not yet considered a model of how trustmarks might interact with the *Privacy Act*, but expressed interest in examining any such proposals, if and when they are put forward.[97] In the view of the Office of the NSW Privacy Commissioner (Privacy NSW), the value of trustmarks is 'dependent on the rigour of the compliance and audit functions which support them'. It submitted that, if it was proposed that the OPC would have power to issue or approve trustmarks, thought should be given to how compliance with a trustmark would be audited and how the complaint process for individuals would work. Privacy NSW also referred to the current discussions in APEC about the use of trustmarks. In its view, these discussions

---

<www.trustsg.com/radiantrust/tsg/rel1_0/html/asiatrust.html> at 6 May 2008; Global Trustmark Alliance, *Website* <www.globaltrustmarkalliance.org> at 6 May 2008.

93 See, eg, TRUSTe, *Website* <www.truste.org> at 6 May 2008.

94 TrustSg, *National Trust Councils & ACOs* <www.trustsg.com/radiantrust/tsg/rel1_0/html/TrustCouncil.html> at 6 May 2008.

95 See, eg, TRUSTe, *Website* <www.truste.org> at 6 May 2008.

96 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 28–2.

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

offered 'some hope of realistic, widely recognised and respected use of trustmarks' and the possibility that APEC itself could be the issuer of trustmarks.[98]

31.64 Other stakeholders expressed strong support for the use of trustmarks. Unisys Asia Pacific, for example, argued that 'there is an opportunity and an imperative to go further'. It submitted that 'steps [should] be taken towards an international privacy standards body' because without this, 'the national privacy framework would be potentially undermined by the lack of internationally consistent standards'.

> Establishing global standards can have a profound social and economic impact through enabling the potential to be realized while ensuring that minimum commonality in approach is maintained. This could be a stand alone organisation, sit within an existing body (such as International Standards Organisation or WTO) or be established by some other construct. Similar to the CEIA, an important end goal of a privacy standards body would be to create a baseline for adoptable global practices in privacy, allowing privacy certifications to operate across international borders and encourage confidence and trust from organisations and individuals across the world.[99]

31.65 Smartnet submitted that trustmarks are important, especially for internet services. It expressed a desire to see some form of trustmark on the websites of all Australian organisations that hold or use large amounts of personal data, particularly those organisations that require people to disclose personal data in order to receive services.[100]

31.66 The Australian Bankers' Association (ABA) also expressed the view that trustmarks should be encouraged if they give confidence to users of e-commerce. It noted that one possibility would be to allow Australian banks to recognise the issue of a trustmark to an overseas entity as an 'authentication' that the overseas entity is subject to a 'law, binding scheme or contract' for the purposes of the UPPs. It submitted, however, that incorporating trustmarks in the *Privacy Act* required further consideration. The ABA stated that the role of a trustmark entity should not overlap with the role of the OPC, 'so that agencies and organisations are not exposed to dual "regulatory" bodies'.[101]

31.67 Similarly, the National Australia Bank, while indicating that it appreciated the effectiveness of trademarks, submitted that further details were required in relation to the proposed scheme. Such details would include which body would administer the scheme, its framework and how the responsibilities of that body would be separated from those of the OPC. It indicated that any such scheme should not detract from the OPC's primary responsibilities which are providing advice to organisations and consumers about privacy laws, and handling complaints.[102]

---

98 Privacy NSW, *Submission PR 468,* 14 December 2007.
99 Unisys, *Submission PR 569,* 12 February 2008.
100 Smartnet, *Submission PR 457,* 11 December 2007.
101 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008.
102 National Australia Bank, *Submission PR 408,* 7 December 2007.

31.68 Some stakeholders disagreed with the proposal. The Public Interest Advocacy Centre (PIAC) was 'unconvinced' by the utility of trustmarks which, in its view, do not provide a sufficient guarantee of privacy protection.[103] The Australian Privacy Foundation submitted that there should be no provision for trustmarks under the *Privacy Act* and the OPC should not be involved with them, unless there is a 'compelling case of value to consumers'.[104] One stakeholder expressed a concern about the effect on privacy protection in Australia when trademarks are issued by companies based in countries where privacy legislation is less robust than in Australia.[105] Another stakeholder submitted that while the idea had merit, it 'would be open to abuse and would therefore require constant enforcement and possibly penalties for false use in order to retain the confidence of the public'.[106]

31.69 In the view of the Office of the Victorian Privacy Commissioner (OVPC):

> The benchmark should be legislation, with strong and effective independent regulators. This will be the case in Australia if the proposed UPPs and regulatory models are adopted and could provide a regional and international model for privacy regulation.
>
> However, in jurisdictions where this benchmark is unable or unlikely to be achieved, alternative arrangements, including the use of trustmarks, could be considered. In my view, current international schemes, such as the APEC Privacy Framework, are not yet sufficiently well developed to be recognised legislatively.[107]

ALRC's view

31.70 The use of trustmarks as a method of promoting compliance with, and enforcement of, the *Privacy Act* and other international privacy regimes should be explored. It is premature, however, to introduce the concept of trustmarks into the *Privacy Act.* The concept needs to be developed further before it would be appropriate for introduction as a mechanism under the *Privacy Act*.

Current coverage of cross-border data flows

Extraterritorial operation of the *Privacy Act*

31.71 Section 5B of the *Privacy Act* applies the Act (and approved privacy codes) to acts done, or practices engaged in, outside Australia by an organisation, if the act or practice relates to personal information about an Australian citizen or permanent resident and either the organisation:

---

103 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
104 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
105 P Youngman, *Submission PR 394*, 7 December 2007.
106 S Hawkins, *Submission PR 382*, 6 December 2007.
107 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

- is linked to Australia by being a citizen; or a permanent resident; or an unincorporated association, trust, partnership or body corporate formed in Australia; or

- carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.

31.72 Section 5B(4) extends the enforcement powers of the Privacy Commissioner to overseas complaints that fall within the criteria in s 5B(1).[108] The purpose of s 5B is to stop organisations avoiding their obligations under the Act by transferring the handling of personal information to countries with lower privacy protection standards.[109] The privacy laws of another country, however, will not be overridden by the *Privacy Act*. Where an act or practice is required by an applicable law of a foreign country, it will not be considered a breach of the *Privacy Act.*[110]

Agencies

31.73 Section 5B applies to organisations, but not to agencies. It is unclear whether, in the absence of an express statement, the *Privacy Act* operates extraterritorially in relation to the acts and practices of agencies. It could be argued that the IPPs apply to the records of Australian Government agencies wherever they may be.

31.74 The High Court has held, however, that in the absence of unambiguous language to the contrary, there is a common law presumption that courts do not read extraterritorial jurisdiction into legislation.[111] This presumption has been held to apply in the case of legislation that applies to agencies.[112] There are a number of examples of federal legislation that regulates the Australian Government public sector and expressly provides that the legislation is to have extraterritorial application.[113]

31.75 The ALRC proposed in DP 72 that the *Privacy Act* be amended to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency.[114]

---

108 The enforcement powers of the Privacy Commissioner are considered in Ch 50.

109 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [1-460].

110 *Privacy Act 1988* (Cth) s 13D.

111 *Jumbunna Coal Mine NL v Victorian Coal Miners Association* (1908) 6 CLR 309.

112 *Brannigan v Commonwealth* (2000) 110 FCR 566. In this case, the appellant worked for the Australian High Commission in London. She complained of breaches of the *Racial Discrimination Act 1975* (Cth), *Sex Discrimination Act 1984* (Cth) and the *Disability Discrimination Act 1992* (Cth) while she was working at the High Commission. The Federal Court of Australia held that it lacked jurisdiction to determine the matter because the Acts did not state expressly that they operated extraterritorially.

113 See *Public Service Act 1999* (Cth) s 5; *Occupational Health and Safety Act 1991* (Cth) s 13(2); *Ombudsman Act 1976* (Cth) s 3C; *Crimes Act 1914* (Cth) s 3A. See *McDonald v Bojkovic* [1987] VR 287.

114 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–1.

Submissions and consultations

31.76 The overwhelming majority of stakeholders supported the ALRC's proposal.[115] In the OPC's view, the *Privacy Act* currently applies to Australian agencies operating outside Australia, however, it submitted that there was merit in amending the *Privacy Act* to clarify this point.[116] The OVPC submitted that, 'in the interests of uniformity, each piece of state or territory legislation should contain a similar provision indicating that it applies to acts done/practices engaged in outside the relevant jurisdiction by a state or territory agency'.[117]

31.77 A number of stakeholders emphasised the need for equivalence between the public and private sectors. For example, the Government of South Australia submitted that 'the privacy protection offered to the public by Governments should be at least equal to the privacy protection required of the private sector'.[118] The Australasian Compliance Institute fully supported the consistent treatment of privacy principles between public and private sector organisations.[119] Also, PIAC's view was that the proposal was important because agencies are frequently able to compel the collection of personal information.[120]

31.78 Some agencies expressed reservations. The Australian Federal Police (AFP) submitted that any extension of the *Privacy Act* to acts or practices by agencies outside Australia may be present compliance and enforcement difficulties.[121]

ALRC's view

31.79 Agencies that operate outside Australia should be subject to the *Privacy Act*. Agencies often compel the collection of personal information and should therefore remain accountable for the handling of that information under the *Privacy Act*, whether

---

115 Unisys, *Submission PR 569*, 12 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 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; Queensland Government, *Submission PR 490*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

117 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

118 Government of South Australia, *Submission PR 565*, 29 January 2008.

119 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

120 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

121 Australian Federal Police, *Submission PR 545*, 24 December 2007.

they are located in Australia or offshore. Further, agencies should not be able to avoid their obligations under the Act by transferring the handling of personal information to entities operating in countries with lower privacy protection standards. The ALRC recommends below that the *Privacy Act* be amended to clarify that it applies to the acts and practices of agencies that operate outside Australia. A similar provision should be included in state and territory legislation.

Information held under the law of a foreign country

31.80 The *Privacy Act* provides that, where overseas acts and practices are required by an applicable foreign law, they are generally not considered interferences with the privacy of an individual.[122] The purpose of s 13D was to ensure that 'the extraterritorial operation of the Act does not require organisations to act in contravention of laws operating in the country in which the act or practice occurs'.[123]

31.81 These acts and practices may be interferences with privacy, however, if they: breach the Tax File Number (TFN) guidelines, or involve an unauthorised requirement or request for disclosure of an individual's TFN; breach Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) or the data-matching guidelines issued under that Act; constitute a breach of the guidelines under s 135AA of the *National Health Act 1953* (Cth); or constitute a credit reporting infringement by a credit reporting agency or a credit provider.[124] One issue raised in this context[125] arose from the debate in Canada about whether information held in the United States might be subject to secret demands under the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (US) (US Patriot Act).[126]

31.82 In 2004, concerns were raised in Canada about whether organisations outside Canada, which were contracted to provide services to the federal and provincial governments, could be required to provide personal information about Canadian

---

122 See *Privacy Act 1988* (Cth) ss 6A(4), 6B(4), 13D(1).

123 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [65], [70].

124 *Privacy Act 1988* (Cth) s 13E.

125 Other concerns raised by stakeholders in relation to information held under the law of a foreign country are discussed in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.14]–[28.20].

126 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007. Other examples include the handing over by Yahoo of a dissident journalist's email account details to the Chinese police in a matter that was the subject of investigation by the Hong Kong Privacy Commissioner; and the US Government mandating the transfer of passenger name records (PNRs) on all incoming international flight passengers. Issues were raised in relation to whether the release of PNRs was permitted under the EU Directive. The US and the EU have recently entered an agreement in relation to processing and transfer of PNRs. See *Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), 23 July 2007*.

citizens to the US authorities.[127] In response to these concerns, the Government of British Columbia amended the *Freedom of Information and Protection of Privacy Act 1996* (British Columbia) to provide that a government agency must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, except in certain circumstances.[128] The Canadian Government, by contrast, did not adopt a legislative approach to this issue. It developed a strategy that involved raising awareness and providing guidance about privacy risks associated with contracting with organisations outside Canada.[129]

31.83 Should the *Privacy Act* limit the circumstances when personal information transferred outside Australia will become subject to a foreign law? One option would be to amend s 13D to provide for certain limits. Another option is that reflected in the Privacy Protection for Off-shoring Bill 2007 (Cth).[130] The Bill sought to amend the *Financial Management and Accountability Act 1997* (Cth) by introducing a new s 43A which would have required an agency entering into a Commonwealth contract for the provision of services in Australia to take contractual measures to ensure that a contracted service provider cannot undertake work in relation to the contract in a country other than Australia that would involve use of 'personally identifiable information'.[131] The Bill reflects one method of protecting personal information from being collected and held under the law of a foreign country.

31.84 The Department of Finance and Deregulation raised concerns about the US Patriot Act. It noted that while Australian government agencies may impose contractual restrictions on service providers transferring confidential or personal information, they may not know that such transfers are or may be taking place under the US Patriot Act and hence will have no knowledge that a possible breach of contract may have occurred.[132]

---

127 See Treasury Board of Canada, *Privacy Matters: The Federal Strategy to Address Concerns About the US PATRIOT Act and Transborder Data Flows* (2006); Information and Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (2004).

128 *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia) s 30.1. The Act also provides that the relevant government minister is to be informed when a government agency or contracted service provider receives a foreign demand for disclosure: *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia) s 30.2.

129 Treasury Board of Canada, *Privacy Matters: The Federal Strategy to Address Concerns About the US PATRIOT Act and Transborder Data Flows* (2006), Ch 3.

130 The Privacy Protection for Off-shoring Bill 2007 was introduced by the Hon Anna Burke MP into the Australian Parliament House of Representatives on 18 June 2007. The Bill also sought to amend the *Trade Practices Act 1974* (Cth).

131 The Privacy Protection for Off-shoring Bill 2007 proposed to introduce a new 65AAAB of the *Trade Practices Act*, which defines 'personally identifiable information' as information including: name, postal address, financial information, medical records, date of birth, phone number, email address, Medicare number, mother's maiden name, driver's licence number and tax file number. Most of this 'information' would be 'personal information' under the *Privacy Act*.

132 Australian Government Department of Finance and Deregulation, *Submission PR 558,* 11 January 2008.

31.85 The ALRC does not recommend that s 13D of the *Privacy Act* be amended to limit the circumstances in which personal information transferred outside Australia will become subject to foreign law. In the ALRC's view, the policy justification for s 13D is sound—acts and practices that take place in a foreign country, and are required by the laws of that country, generally should not be considered a breach of the Act. It would not be workable to prevent the transfer by agencies and organisations of personal information to countries such as the US. Also, it would be unfair to render an agency or organisation transferring personal information under s 13D responsible for an act or practice of the recipient which is required by a foreign law, when neither they, nor the recipient, can control or prevent the acts or practices required under such a foreign law.

31.86 The OPC's guidance on the recommended 'Cross-border Data Flows' principle should set out the steps to be taken when personal information transferred outside Australia may become subject to a foreign law, including laws such as the US Patriot Act. The guidance also should provide advice to agencies when contracting government services to organisations outside Australia.

National Privacy Principle 9

31.87 NPP 9 dictates the circumstances in which an organisation may transfer personal information it holds in Australia to someone in a foreign country. As with the other private sector provisions, it was introduced in 2000 as part of the extension of privacy principles to the private sector.[133]

31.88 NPP 9 prohibits the transfer by an organisation of an individual's personal information to someone in a foreign country (other than that individual or organisation) unless a number of conditions are satisfied.[134]

31.89 The principle is largely modelled on arts 25 and 26 of the EU Directive, which aim to ensure continued protection of personal information when data are sent from their originating country.[135] Where one of the conditions in (a)–(f) is satisfied, the Australian organisation transferring the data is not liable for subsequent privacy breaches.

31.90 NPP 9 is limited to 'foreign countries' rather than 'other jurisdictions'. It does not protect personal information that is transferred to a state or territory government that is not subject to privacy law, or a private sector organisation that is exempt from

---

133 N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39, 42.

134 G Greenleaf, 'Exporting and Importing Personal Data: The Effects of the Privacy Amendment (Private Sector) Bill 2000' (Paper presented at National Privacy and Data Protection Summit, Sydney, 17 May 2000), 7.

135 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58; N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39.

the *Privacy Act*.[136] Where the transfer of personal information overseas is to the same organisation, not a third party, NPP 9 does not apply.

31.91 The *Privacy Act* was amended in 2004 to make it clear that the protection provided by NPP 9 applies equally to the personal information of Australian and non-Australian individuals.[137] This amendment was made by excluding NPP 9 from the citizenship and residency requirements of s 5B(1).

31.92 In IP 31, the ALRC asked whether NPP 9 provides adequate and appropriate protection for personal information transferred from Australia to a foreign country.[138] While some stakeholders submitted that the protection afforded by NPP 9 was sufficient, others noted that NPP 9 is deficient in a number of respects, including: that organisations transferring data are not liable for any subsequent breaches; the perceived weakness of the tests for a 'reasonable belief' (NPP 9(a)); the operation of consent in the context of cross-border data flows; the failure to address the transfer of personal information offshore by agencies; a lack of clarity as to how NPP 9 relates to other parts of the *Privacy Act*; and a lack of guidance for organisations as to what steps they must take to comply with NPP 9.[139] Each of these criticisms, along with the ALRC's recommended approach, is dealt with in detail below.

Content of the model 'Cross-border Data Flows' principle

Accountability

31.93 Professor Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that the six conditions under NPP 9 will generally be sufficient to allow any legitimate transfer overseas of personal information, even when those transfers may harm the interests of the data subjects concerned. They argued that data exporters should remain liable for breaches of privacy by data importers under most circumstances.[140]

31.94 Unisys submitted that:

> As a leading provider of outsourced services in Australia and internationally, it is our experience that there is a gap between public perception and operational reality in the way that business and government treat personal information. Organisations are investing heavily to ensure that data is secure, whether handled directly or by third parties, whether onshore or offshore—including in physical and enterprise security, as well as HR/Hiring policies. Stipulating liability for information sent overseas would

136 N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39.

137 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [1-460].

138 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–1.

139 Stakeholder views on this issue were canvassed in detail in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.28]–[28.31], [28.48], [28.52], [28.55], [28.60], [28.63]–[28.64].

140 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

> also encourage greater transparency on the measures that are planned and in place. Governments and commercial enterprises have an imperative to build confidence amongst the citizens and customers with whom they interact.[141]

31.95 One option is to amend the *Privacy Act* to introduce an 'accountability' concept in the proposed 'Cross-border Data Flows' principle. In DP 72, the ALRC suggested that this could be achieved by providing that agencies and organisations will continue to be liable for any breaches of the proposed UPPs when an individual's personal information is transferred outside Australia.

Accountability under APEC

31.96 The APEC Privacy Framework provides that, when transferring personal information, a 'personal information controller' should be accountable for the protection of that personal information consistently with the APEC Privacy Principles, even if the information moves from one jurisdiction to another.[142] The Commentary on Principle 9 states:

> When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed. In these types of circumstances, personal information controllers may choose to use other means, such as obtaining consent, to ensure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations.[143]

31.97 Margaret Eisenhauer stated that 'APEC approach-based laws will recognise that global data flows are facilitated if the laws focus on ensuring that local companies are accountable for data processing activities'.[144] Gehan Gunasekara discusses the 'hiatus' in current privacy regulation and argues:

> The principles as to onward transfer are, of necessity, open-ended. They point to the imperative for proactive measures to be adopted in future to close any privacy loopholes and lead inexorably to cross-jurisdictional paradigms. Far from being a solution, the existing jurisdictional approaches are therefore merely a pointer to future developments.[145]

---

141 Unisys, *Submission PR 569*, 12 February 2008.
142 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 9.
143 Ibid, Principle 9 (commentary).
144 M Eisenhauer, *Privacy and Security Law Issues in Off-Shore Outsourcing Transactions* (2005) Hunton & Williams, 5.
145 G Gunasekara, 'The "Final" Privacy Frontier? Regulating Trans-border Data Flows' (2006) 15 *International Journal of Law and Information Technology* 362, 382.

31.98 While the APEC Privacy Framework introduces the principle of accountability, as discussed above, its approach to cross-border implementation is flexible. The Framework states that 'the means of giving effect to the Framework may differ between Member Economies'.[146] Member Economies are encouraged to 'share experiences on various techniques in investigating violations of privacy protections and regulatory strategies'.[147] Emphasis also is placed on cross-border cooperation in investigation and enforcement.[148] Australia is taking a lead role in APEC Data Pathfinder Projects to develop co-mechanisms for such cooperation, as discussed above.[149]

Accountability under the model 'Cross-border Data Flows' principle

31.99 To what extent should agencies and organisations remain liable when transferring personal information outside Australia? The approach to accountability under the APEC Privacy Framework is innovative in that it is based on the idea that 'accountability should follow the data'.[150] The flexibility in its approach to cross-border implementation may mean that currently, in practice, the framework cannot deliver a sufficient level of protection for Australians in relation to cross-border data flows. Of particular relevance is Greenleaf's objection to the 'non-prescriptive' approach to the implementation aspects of Part IV of the Framework which, he says, 'exhort[s] APEC members to implement the Framework without requiring any particular means of doing so, or any means of assessing whether they have done so'.[151]

31.100 As discussed above, there are currently no data protection laws in key economies such as India and China.[152] Further, India is not a member economy of APEC.[153] Robertson states, in relation to China, that:

> China's response to the APEC Privacy Framework has not been positive, and China is not participating in the APEC Data Privacy Pathfinder program, although the reasons for this are not clear.[154]

---

146 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [32].

147 Ibid, [42].

148 Ibid, [44]–[45].

149 K Curtis, 'Information Workshop for Australian Stakeholders' (Paper presented at APEC Data Privacy Pathfinder Seminar, Sydney, 6 February 2008), 5–9.

150 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8.

151 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121, 122.

152 B Cruchfield George and D Roach Gaut, 'Offshore Outsourcing to India by EU and US Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing' (2006) 6 *University of California Business Law Journal* 13, 13; S Robertson, 'Offshore Business Processing in China Brings Privacy Concerns' (2008) 10 *Internet Law Bulletin* 118, 118.

153 Asia-Pacific Economic Cooperation, *Member Economies* (2008) <www.apec.org/content/apec/member_economies.html> at 22 April 2008.

154 S Robertson, 'Offshore Business Processing in China Brings Privacy Concerns' (2008) 10 *Internet Law Bulletin* 118, 119. See also G Greenleaf, 'A Tentative Start for Implementation of APEC's Privacy Framework' (2005) *Privacy Law and Practice Reporter* 16, 16.

31.101 It is important that the personal information of Australians is protected adequately when it is subject to cross-border transfer. Svantesson argues for a model of strict liability for data exporters.[155] He argues that 'by imposing this liability, it can be anticipated that data exporters will take greater care in selecting to whom they will export personal information'.[156] Similarly, Professor Fred Cate notes that:

> Users of personal information—whether in the public or private sectors—frankly are not very interested in meaningful, third-party accountability …
>
> The absence of rational, effective accountability systems undermines privacy and consumer confidence.[157]

31.102 It has been suggested that the conception of privacy as a 'key reputational risk' is an important consideration for organisations.[158] Commentators on business ethics have noted that 'somehow we need to determine who is responsible for business practices, both commendable and questionable ones'.[159]

31.103 Also relevant is Blair Stewart's observation about the way in which individuals typically make complaints and the factors which may impact on the progress of such complaints.

> Instinctively, the individual may complain to the local institution with which he or she is most familiar. That enforcement authority may consider the complaint to be outside its jurisdiction. In such a case, does it consult an overseas authority on the complaint and transfer it? Or does it simply notify the complainant that it is beyond its jurisdiction and suggest that the individual take the matter up elsewhere?
>
> The scenario might also be complicated if either jurisdiction has no enforcement authority or if the authority in the other jurisdiction is of a different kind (such as a web seal programme or self regulatory body). These problems are by no means insurmountable but there is a considerable likelihood that the complications and difficulties will discourage either the local authority from taking any steps at all or leave the individual unable to obtain meaningful redress.[160]

Discussion paper proposal

31.104 In DP 72, the ALRC proposed the introduction of the concept of accountability into the 'Cross-border Data Flows' principle, linking it to clauses (c)–(f) of NPP 9. In developing the blended proposal, the ALRC modified existing clauses (c) and (f) of NPP 9 to address concerns raised by stakeholders.[161]

---

155 D Svantesson, 'Protecting Privacy on the "Borderless" Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168, 183–184.

156 Ibid, 184.

157 F Cate, 'Security and Privacy Challenges in the Decade Ahead' (2006) 6(12) *IAPP* 1, 20.

158 S Kenny, 'Global Privacy Predictions for 2008' (2008) 8(1) *Privacy Advisor* 11, 11.

159 R Buchholz and S Rosenthal, 'Integrating Ethics All the Way Through: The Issue of Moral Agency Reconsidered' (2006) 66 *Journal of Business Ethics* 233, 233.

160 B Stewart, 'Cross-Border Cooperation on Enforcement Matters' (2005) *Privacy Law & Policy Reporter* 2, 5.

161 NPP 9.1(a) and (b) are discussed below under the headings 'Substantially similar privacy protections' and 'Consent'.

31.105 The ALRC proposed that NPP 9(c) be amended to provide that the transfer of personal information overseas, where necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, should be within the 'reasonable expectations' of the individual. The ALRC also proposed that NPP 9(f) be amended to require that *before* a transfer takes place, an agency or organisation must take reasonable steps to ensure that the information will not be handled by the recipient of the information inconsistently with the proposed UPPs. The ALRC did not propose any changes to clauses NPP 9(d) and (e).[162]

31.106 In DP 72, the accountability limb of the 'Cross-border Data Flows' principle proposed by the ALRC provided that an agency or organisation in Australia or an external territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia if:

> (c) the agency or organisation continues to be liable for any breach of the proposed UPPs; and
>
> (i) the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation;
>
> (ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;
>
> (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;
>
> (iv) all of the following apply: the transfer is for the benefit of the individual; it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or
>
> (v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs.[163]

---

162 Stakeholder views on clauses NPP 9 (c)–(f), and the reasons for the ALRC's proposals, were canvassed in detail in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.51]–[28.62].

163 Ibid, Proposal 28–4.

Submissions and consultations

31.107 A number of stakeholders supported the introduction of the concept of accountability into the 'Cross-border Data Flows' principle.[164] The Department of Broadband, Communications and the Digital Economy noted that the proposed accountability concept 'would go some way to addressing the issue' it had raised previously; namely, the 'inherent difficulties in imposing legal responsibility upon an overseas recipient of personal information to use or disclose that personal information in a manner that is consistent with NPPs'. It noted that the onus would be on the agency or organisation to mitigate their liability in contractual arrangements with the recipient of personal information.[165]

31.108 The Cyberspace Law and Policy Centre expressed its support for the concept of data exporters remaining liable, which in its view was a 'significant' change.[166] Another stakeholder noted the difficulty for individuals of pursuing their privacy rights in foreign countries, in particular, that there is often no way to verify compliance.[167] The Australasian Compliance Institute pointed out that, currently, the *Privacy Act* may not allow for situations where a third party is appointed to undertake services and outsources to another third party, who may be an overseas service provider.[168]

31.109 There was also a significant amount of opposition to the proposed introduction of accountability, particularly from organisations.[169] A number of stakeholders argued that the protection afforded by NPP 9 was adequate.[170]

31.110 The ABA raised questions about the potential operation of an accountability concept under the *Privacy Act.*

> It is unclear how the organisation can remain liable for breaches of the UPPs by a third party when that third party is not bound by UPPs and therefore incapable of breaching them. It is unclear whether the organisation is to continue to be liable for any breaches of the UPPs pursuant to its contract with the data subject or if the

---

164 Unisys, *Submission PR 569,* 12 February 2008; Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Confidential, *Submission PR 535,* 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; Centre for Law and Genetics, *Submission PR 497,* 20 December 2007; Queensland Government, *Submission PR 490,* 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; National Health and Medical Research Council, *Submission PR 397,* 7 December 2007.

165 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512,* 21 December 2007.

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

167 Confidential, *Submission PR 535,* 21 December 2007.

168 Australasian Compliance Institute, *Submission PR 419,* 7 December 2007.

169 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; GE Money Australia, *Submission PR 537,* 21 December 2007; Confidential, *Submission PR 536,* 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525,* 21 December 2007; ANZ, *Submission PR 467,* 13 December 2007; Microsoft Asia Pacific, *Submission PR 463,* 12 December 2007.

170 GE Money Australia, *Submission PR 537,* 21 December 2007; Confidential, *Submission PR 536,* 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525,* 21 December 2007.

> legislation is to impose this liability. The ABA assumes that the former is the case so that the voluntary assumption of liability by the transferor organisation by contract with the individual concerned would trigger the exceptions in sub-paragraphs (i) to (iv) that appear to be written disjunctively…
>
> Further, if the legislation imposed liability on an organisation for a transborder third party's breach of the UPPs independently of contract, it is unclear why any of the circumstances as set out in sub-paragraphs (i) to (v) are necessary because the organisation would be liable in any event.[171]

31.111 In the ABA's view, a transferor organisation should be able to 'resist liability if it can show it did not act irresponsibly in initiating the transfer'. The ABA noted that the proposal did not provide any scope for the transferor to advance any defence to liability.[172]

31.112 GE Money also disagreed with the proposal, stating that it should be 'sufficient that an organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs'.[173] One stakeholder strongly objected to the proposal that an organisation be liable for 'downstream breaches' on the basis that 'such a condition would be unfair, inappropriate and impractical and would have arbitrary effects'.[174]

31.113 In ANZ's view, while the proposal would preserve its ability to send personal information about an individual offshore, it would be unreasonable for an organisation to continue to be liable for breaches of the UPPs by a third party. ANZ submitted that, where third party breaches occur, 'flexibility should be retained (determined by the relevant contract)' as to whether the organisation, or third party, should be responsible for 'determining whether the breach is capable of causing serious harm' and 'completing notification procedures'.[175]

31.114 Microsoft submitted that the proposed UPP was less conducive to the free flow of information than NPP 9, because it required regulated entities to satisfy the APEC notion of accountability, in addition to some of the existing conditions in NPP 9. It submitted, however, that:

> Microsoft's view is that the APEC notion of accountability alone is sufficient to regulate transborder data flows. Put another way, there is no need to include conditions of transfer such as those set out in … (i) to (v) … if the organisation transferring the personal information remains accountable for the data. In Microsoft's opinion, the APEC notion of accountability helps to assuage individuals' concerns

---

171 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008. See also: GE Money Australia, *Submission PR 537*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

172 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

173 GE Money Australia, *Submission PR 537*, 21 December 2007. Also: Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

174 Confidential, *Submission PR 536*, 21 December 2007.

175 ANZ, *Submission PR 467*, 13 December 2007.

> regarding offshore transfers of their personal information without imposing unnecessary burdens on transborder data flows. Such an approach also provides organisations with the flexibility to decide how they comply with this requirement, while still providing the individual with an appropriate level of privacy protection.
>
> Microsoft therefore urges the ALRC to reconsider its proposed approach to the regulation of transborder data flows having regard to the crucial goal of harmonisation with international instruments such as the APEC Privacy Framework.[176]

31.115 Some agencies raised particular concerns. The Department of Foreign Affairs and Trade (DFAT) suggested that an exception similar to that in the proposed 'Use and Disclosure' principle be included in the 'Cross-border Data Flows' principle, namely where: use or disclosure is reasonably necessary to prevent a threat to life or health or safety; or public health or public safety. DFAT stated that it often 'encounters cases where the disclosure of personal information would benefit a third party rather than the individual concerned'.[177] An example of this is where DFAT is asked to provide information to foreign authorities in relation to an Australian national if there are concerns regarding that person's capacity to care for his or her children. The Department of Defence noted that Australia is committed to operational deployments and joint military exercises with a number of foreign governments. It submitted that disclosure of information to foreign forces is required in order to support these engagements, but that the proposal did not seem to have application in this context.[178]

31.116 Some stakeholders addressed the drafting of particular limbs of the accountability clause. The Cyberspace Law and Policy Centre noted that the conditions in proposed clause (c)(i)–(iv) were not contentious because they were similar to those in art 26(1) of the EU Directive. It supported the use of the term 'reasonable expectations' of the individual in proposed clause (c)(i) and (ii), on the basis that it would make it more likely that agencies and organisations will make the likelihood of overseas transfers subject to explicit notice.[179] Another stakeholder, however, objected to the addition of the 'reasonable expectations' test in relation to the performance of contracts.[180]

31.117 Regarding the requirement in proposed clause (c)(iv) that 'consent would be likely to be provided', one stakeholder submitted that often others interpreted that phrase 'in their favour and against my own wishes known and unknown'.[181] PIAC also opposed proposed clause (c)(iv), on the basis that an agency or organisation should not be able to presume that a cross-border transfer is for the benefit of an individual or that an individual would be likely to consent.[182] One stakeholder argued that the requirements relating to the 'interests of' or 'benefits of' individuals should not be

---

176 Microsoft Asia Pacific, *Submission PR 463,* 12 December 2007.
177 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563,* 24 January 2008.
178 Australian Government Department of Defence, *Submission PR 440,* 10 December 2007.
179 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.
180 Confidential, *Submission PR 536,* 21 December 2007.
181 Confidential, *Submission PR 535,* 21 December 2007.
182 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

retained. The stakeholder argued that this is a judgment that is extremely difficult for an organisation to make and called for clearer criteria.[183] Privacy NSW supported the ALRC's proposal, but submitted that an objective test regarding the 'benefit of the individual' should be included in the model UPP or, alternatively, that the OPC should provide guidance as to when a transfer would benefit the individual.[184]

31.118 PIAC and the Cyberspace Law and Policy Centre expressed support for the requirement in proposed clause (c)(v), that an agency or organisation must take steps *before* a transfer takes place.[185] The Cyberspace Law and Policy Centre argued, however, that proposed clause (c)(v) should not be seen as alternative basis for transfer—instead, it should apply to all transfers, other than those covered by proposed clause (a), relating to substantially similar privacy protections.[186] The ABA submitted that there was an 'uncertain relationship' between proposed clause (a) and clause (c)(v) which needed to be clarified. In the ABA's view, it should be clear that the transferor's knowledge of the existence of an overseas regime similar to the *Privacy Act* should be sufficient to satisfy clause (c)(v).[187]

ALRC's view

31.119 In line with principles-based regulation, and to ensure consistency with the other model UPPs, the ALRC recommends the introduction of a general principle of accountability in the 'Cross-border Data Flows' principle. In DP 72, the proposal linked accountability to a range of elements which currently form part of NPP 9. In the ALRC's view, if organisations are to remain liable, these elements are superfluous and do not provide a greater level of privacy protection. The principle recommended by the ALRC has been streamlined to strip away these elements. It also responds to stakeholder views that accountability should operate more simply under the 'Cross-border Data Flows' principle.

31.120 Accountability should operate as the default position in relation to cross-border transfers of personal information. This policy position is warranted both by the high level of community concern attaching to cross-border transfers of personal information and the nature of the risks associated with such transfers. The benefit of this approach is that it does not prevent information from being transferred. Instead, it requires agencies and organisations to remain responsible for personal information when transferred. There are three circumstances, however, when an agency or organisation should not remain accountable. These are when the:

---

183 Confidential, *Submission PR 536*, 21 December 2007.
184 Privacy NSW, *Submission PR 468*, 14 December 2007.
185 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
186 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. Note: clause (a) reproduces NPP 9(a).
187 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

- information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the UPPs;

- individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

- agency or organisation is required or authorised to transfer the personal information by or under law.

31.121 This will allow, for example, agencies and organisations to mitigate their liability through contractual arrangements with the recipient of the personal information. These exceptions also will address the concerns of agencies discussed above.

31.122 The ALRC's recommended approach to accountability under the 'Cross-border Data Flows' principle draws on the APEC concept of accountability, but takes it further. As Greenleaf argues, the APEC Privacy Framework is 'a floor not a ceiling'.[188] The ALRC's recommended approach provides for an agency or organisation to remain responsible under Australian privacy law in respect of the actions taken by a recipient of personal information outside Australia. Placing responsibility on the agency or organisation transferring the personal information ensures that an individual has the ability to seek redress from someone in Australia if the recipient breaches the individual's privacy. Further, the individual will be able to approach a local regulator, rather than have to seek protection under a foreign law, which may not provide the same level of protection as a local law.[189]

31.123 The general principle of accountability should mean that an agency or organisation will be responsible under the *Privacy Act* for the acts and practices of a recipient of personal information the subject of a cross-border transfer. That is, where an agency or organisation transfers information to a recipient outside Australia, if the acts or practices of that recipient in respect of the personal information would have amounted to an interference with the privacy of an individual if done in Australia, they should constitute an interference with the privacy of individual for the purposes of the *Privacy Act*. Further, the acts or practices of the recipient should be taken to be the acts or practices of the relevant agency or organisation for the purposes of the *Privacy Act*.

31.124 This approach gives substance to the general principle of accountability. It will trigger the complaint and investigation mechanisms under Part V of the *Privacy Act*

---

188 G Greenleaf, 'A Tentative Start for Implementation of APEC's Privacy Framework' (2005) *Privacy Law and Practice Reporter* 16, 19.

189 See D Svantesson, 'Protecting Privacy on the "Borderless" Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168, 183–184.

and so provide access to remedies such as a declaration that the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by a complainant, or a declaration that a complainant is entitled to a specified amount of compensation.[190] Consequential amendments to Division 1 of Part III of the *Privacy Act* also may be required.

31.125 The ALRC's recommended approach to accountability is consistent with the APEC preamble[191] and the success criteria for the APEC Privacy Framework.[192] Also, the recommended exceptions to the general principle of accountability are in line with the commentary on Principle 9 of the APEC Privacy Framework.[193] Similarly, APEC's mechanisms for investigation[194] are consistent with the ALRC's model of accountability. They are conducive to the effective operation of the general principle of accountability, in that cross-border cooperation will be required to facilitate the investigation of incidents occurring outside Australia.

31.126 The limbs of the 'Cross-border Data Flows' principle recommended by the ALRC are now addressed in turn.

Substantially similar privacy protections

'Reasonably believes'

31.127 NPP 9(a) states that an organisation may transfer personal information to someone overseas where it 'reasonably believes' the recipient is subject to a law, binding scheme or contract that effectively upholds principles substantially similar to the NPPs. In contrast, art 25 of the EU Directive provides that the country in question *must have* an adequate level of protection. Greenleaf has noted that NPP 9 only requires that an organisation reasonably believes that the foreign country has an arrangement that 'effectively upholds' privacy principles, not that there are enforcement mechanisms that are substantially similar to the *Privacy Act*.[195]

31.128 The OPC Guidelines to the NPPs state, in relation to NPP 9:

> Given that transferring personal information overseas may remove it from the protection of Australian law, an organisation relying on NPP 9(a) … may need to be in a position to give evidence about the basis on which it decided that it has met the requirement of 'reasonable belief' …

---

190 *Privacy Act 1988* (Cth) s 52(1).

191 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Preamble.

192 *Report of Second Technical Seminar on International Implementation of the APEC Privacy Framework, Cairns, Australia, 25–26 June 2007*, APEC Paper 2007/SOM3/ECSG/011 (2007), 2.

193 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 9 (commentary).

194 Ibid, [42], [44]–[45].

195 G Greenleaf, 'Exporting and Importing Personal Data: The Effects of the Privacy Amendment (Private Sector) Bill 2000' (Paper presented at National Privacy and Data Protection Summit, Sydney, 17 May 2000), 8.

> Getting a legal opinion would be a good way for an organisation to get such evidence.[196]

31.129 The ALRC did not propose amendment of the 'reasonable belief' test in DP 72. Instead, it proposed that the Australian Government publish a list of laws and binding schemes for the fair handling of personal information that are substantially similar to the proposed UPPs.[197] The ALRC also proposed that the OPC should publish guidance on what constitutes a 'reasonable belief'.[198]

Submissions and consultations

31.130 There was some stakeholder support for the retention of the current condition in NPP 9(a).[199] For example, the Australian Collectors Association stated that it provides the consumer protection necessary to ensure appropriate handling of personal information.[200] The National Australia Bank submitted that, for the purposes of the ALRC's proposed clause (a), reliance on the list detailed in DP 72[201] should constitute a 'reasonable belief'.[202]

31.131 Some stakeholders expressed reservations.[203] The Australasian Compliance Institute, for example, submitted that because the terminology 'reasonably believes' in clause (a) is open to interpretation, robust guidance on what constitutes 'reasonably believes' should be available.[204] PIAC submitted that the test is ambiguous, and is unlikely to be explained by OPC guidance. PIAC preferred the formulation adopted in the EU Directive, namely that the country to which information is to be transferred must have an adequate level of protection. Alternatively, there should be an explanation in the Act or regulations of what constitutes 'reasonably believes'. PIAC also submitted that the term 'effectively upholds' needs clarification—it should not include self-regulatory schemes.[205]

31.132 One stakeholder disagreed with the ALRC's proposed clause (a) on the basis that 'believing is not quite the same thing as knowing'. The stakeholder claimed that clause (a) was

---

196 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58. See also J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2–5795].

197 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–8.

198 Ibid, [28.50].

199 Australian Collectors Association, *Submission PR 505*, 20 December 2007; Confidential, *Submission PR 536*, 21 December 2007.

200 Australian Collectors Association, *Submission PR 505*, 20 December 2007.

201 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–8.

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

203 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Confidential, *Submission PR 535*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

204 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007. See also Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

205 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

> not good enough … Also other countries interpret some basic standards differently. What would be considered entrepreneurial competitiveness in some parts of the world would be considered unethical, cheating or bribing behaviour in Australia.[206]

31.133 DFAT stated that it is often required to disclose personal information to persons or bodies located overseas.

> In many situations the Department would be unable to state with assurance that the information disclosed would be handled in accordance with a law or scheme which would uphold principles similar to those in the Privacy Act. In such situations, where the transfer of information is beneficial to the individual (where he or she may be detained or receiving medical treatment overseas and it is not possible to obtain his or her consent), the Department should not have to remain liable for breaches of any of the UPPs.[207]

31.134 The Australian Communications and Media Authority (ACMA) was concerned about the 'practicality and reasonableness' of the term 'reasonable belief', in the context of its international anti-spam information-sharing activities. Also, the 'speed with which spammers can relocate operations often means that enforcement agencies and regulators have limited time for effective information-sharing'. ACMA submitted:

> If the proposed conditions were introduced, ACMA may be placed in a position of having to undertake extensive analysis of the law of those countries before it could share information. The practical outcome of these conditions would be that such information-sharing would rarely occur, as the extended timeframe in which the conditions could be met would mean that the utility of the information would have expired by the time the conditions had been fulfilled.[208]

31.135 On the other hand, the Department of Families, Housing, Community Services and Indigenous Affairs submitted that proposed clause (a) was reasonable and, for this reason, did not expect that it would present any substantive issues for it, or for management of programs and data by their business partners in Centrelink.[209]

ALRC's view

31.136 It should be an exception to the default position of accountability if the agency or organisation transferring the personal information outside Australia reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model UPPs.

---

206 Confidential, *Submission PR 535*, 21 December 2007.
207 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.
208 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.
209 Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008.

31.137 The ALRC does not recommend that any change be made to the 'reasonable belief' test. It does recommend, however, that the Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the model UPPs.[210] This will go a long way to creating certainty about when the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles substantially similar to the NPPs. It will address the resource implications for agencies and organisations who currently must undertake such inquiries independently.

31.138 The question of whether the test of 'reasonable belief' is satisfied, however, may involve considerations relating to the level of enforcement of a relevant law, binding scheme or contract, which may not be answered solely by their inclusion on the proposed list. This is implicit in the term 'effectively upholds'. For example, if a country is included on the relevant list as having laws with a substantially similar level of privacy protection, but an organisation is aware that there is no mechanism for enforcement of those laws, it may be that the organisation could not demonstrate a 'reasonable belief' for the purposes of the 'Cross-border Data Flows' principle. This is not to say that an agency or organisation always needs to make inquiries about the mechanisms for enforcement of privacy laws in other jurisdictions, but rather that the question of whether an agency or organisation has a 'reasonable belief' may involve considerations other than whether the relevant law, binding scheme or contract is on the proposed list. This question will need to be resolved on a case-by-case basis.

31.139 The OPC's guidance on the recommended 'Cross-border Data Flows' principle should include guidance on what constitutes a 'reasonable belief'.[211] Obtaining legal advice is one way this requirement could be satisfied.

31.140 The ALRC acknowledges the concerns raised by some stakeholders, in relation to this aspect of the principle, that they may be required to transfer personal information to jurisdictions outside Australia, but are unable to state with assurance that such jurisdictions offer substantially similar privacy protection. The 'required or authorised by or under law' exception, discussed below, will allow agencies and organisations to transfer personal information where required or authorised by or under law to do so, thereby removing the need for them to rely on proposed clause (a) in many instances. In any case, the 'Cross-border Data Flows' principle recommended by the ALRC would not prevent the information being transferred by agencies. Rather, its effect would be that such agencies would remain responsible under the *Privacy Act* for the handling of that personal information after transfer.

---

210 Rec 31–6.
211 Rec 31–7.

Consent

31.141 A number of commentators have raised concerns about the operation of consent in the context of cross-border data flows.[212] Professor Peter Blume argued that, 'in connection with a particular transfer it will often be doubtful whether the data subject can be sufficiently informed and thereby able to fully understand the consequences of consent'.[213] Gunasekara states:

> In any event, it is trite to say that informed consent is necessary. However, consent cannot be truly informed unless the data subject is aware, at the outset, of all the downstream uses to which the information will be put, making it difficult at least to use this as the basis for allowing the transfer of data overseas.[214]

31.142 Svantesson argues that the greatest weakness of NPP 9 arises out of the approach to consent in the *Privacy Act*—'to put it bluntly, consent is the miracle cure that cures virtually any abuse possible under the NPPs'.[215] While he notes that this approach has 'logical appeal' and is probably based in the 'law seeking to provide for party autonomy', he argues it is 'fundamentally flawed'.[216] In Svantesson's view, consent to cross-border data flows is 'rarely sufficiently informed'.[217] He argues that an individual needs to know the country to which their personal information is to be transferred in order to provide informed consent.

31.143 Svantesson refers to the case of *E v Money Transfer Services* as an illustration of the 'weakness of the consent requirement', noting that it is the only reported decision of the OPC that deals with this aspect of NPP 9.[218] In that case, the complainant sought to send Australian currency to their family using a money transfer service. That money transfer service was incorporated in a foreign country and was subject to a subpoena issued by a regulatory body in that country. Under the subpoena, the service was required to provide customer information to the regulatory body, if an individual's name matched a list of 'persons of interest'. The complainant's name matched a name on that list. The money transfer service contacted its Australian subsidiary and asked for further personal information (such as the complainant's driver's licence and passport details) for the purposes of identity verification. The complainant was advised both that the transaction had been halted and of the purpose

---

212 D Svantesson, 'Protecting Privacy on the "Borderless" Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168, 182–3; G Gunasekara, 'The "Final" Privacy Frontier? Regulating Trans-border Data Flows' (2006) 15 *International Journal of Law and Information Technology* 362, 381; P Blume, 'Transborder Data Flow: Is There a Solution in Sight?' (2000) 8(1) *International Journal of Law and Information Technology* 65, 71.

213 P Blume, 'Transborder Data Flow: Is There a Solution in Sight?' (2000) 8(1) *International Journal of Law and Information Technology* 65, 71.

214 G Gunasekara, 'The "Final" Privacy Frontier? Regulating Trans-border Data Flows' (2006) 15 *International Journal of Law and Information Technology* 362, 381.

215 D Svantesson, 'Protecting Privacy on the "Borderless" Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168, 182.

216 Ibid, 182.

217 Ibid, 183.

218 Ibid.

for which he or she needed to provide the further information before the transaction could proceed. The Privacy Commissioner determined that, as the complainant provided the necessary documentation on an informed basis—that is, the complainant was aware that the information would be disclosed to the foreign money service—the complainant's consent to the transfer could be implied from the complainant's actions and the transfer did not breach NPP 9.[219]

31.144 In DP 72, the ALRC did not propose a change to the consent requirement in relation to cross-border data flows specifically. It did address consent as it operates generally under the *Privacy Act*, however, and proposed that the OPC provide guidance about what is required of agencies and organisations to obtain an individual's consent.[220]

Submissions and consultations

31.145 Stakeholders who commented on this issue generally called for tighter requirements with respect to consent. PIAC noted, in this context, the high level of concern among Australians about their personal information being transferred outside Australia.[221] A number of stakeholders submitted that the reference to 'consent' should include only express consent, not implied or bundled consent, particularly as consent absolves the relevant agency or organisation from liability.[222] The OVPC submitted that consent should be express in relation to the 'specific possibility' of cross-border data flows.[223]

31.146 In addition, a number of stakeholders called for informed consent[224] and submitted that in order for consent to be fully informed, an individual should be advised of the countries to which information is to be transferred and the fact that the transferor is disclaiming liability by using the 'consent' exemption.[225] The Cyberspace Law and Policy Centre submitted:

> Another major flaw in the proposed consent exception is that the ALRC anticipates that it would relieve the agency or organisation from any liability for how the information is handled overseas. This approach completely overlooks the fact that

---

219 *E v Money Transfer Service* [2006] PrivCmrA 5.

220 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 16–1.

221 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

222 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

223 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

224 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Confidential, *Submission PR 535*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

225 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

> individuals will typically have absolutely no capacity to sensibly assess the risks associated with transborder data flows. [226]

31.147 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre also argued that the consent exemption should be conditional upon the obligation in clause (c)(v), discussed above in relation to accountability, that, before transfer, reasonable steps be taken to ensure that data will be protected.[227]

31.148 Some stakeholders expressed an alternative view. For example, the ABA submitted that the ability to infer consent should be built into the 'Cross-border Data Flows' principle.[228] Another stakeholder noted that, if a general principle of accountability was implemented, it would 'where possible, seek to rely on the consent exception in relation to the transfer of personal information outside Australia so as to minimise its liability for any breaches of the UPPs outside Australia'. The stakeholder noted, however, that it is not always practical to obtain consent, nor is it always clear whether a person has consented to a particular transfer of personal information to someone outside Australia. It submitted that, to ensure compliance with the consent exemption, extensive disclosure may be required.[229]

ALRC's view

31.149 In Chapter 19, the concept of consent is discussed in detail, including the necessary elements of consent and the issues associated with 'bundled consent'. 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.[230] The cross-border transfer of personal information provides one such context. Any bundled consent obtained should allow the individual to decide whether to consent to the cross-border transfer of their personal information. OPC Guidance relating to bundled consent should specifically address the mechanism of 'bundled consent' in relation to cross-border data flows.[231]

31.150 As noted in Chapter 19, the requisite elements of consent are that it be voluntary and informed. Under the recommended 'Cross-border Data Flows' principle, consent not only permits personal information to be transferred, it takes the individual's personal information outside the default position of accountability under the recommended principle. For this reason, more detailed consent requirements may be justified. For consent to be informed in this context, an individual should be made aware of the legal consequences of providing consent. In order for an agency or organisation to be able to demonstrate that informed consent was obtained, it may be

---

226 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
227 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
228 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.
229 Confidential, *Submission PR 536*, 21 December 2007.
230 Rec 19–1.
231 Rec 19–1.

advisable, where practicable, for the agency or organisation to seek a written acknowledgement from the individual in this regard.

31.151 Informed consent also requires that an individual be advised of the countries to which their information may be sent. The ALRC recommends that an organisation's Privacy Policy include this information.[232] The requirements under the 'Notification' principle in the model UPPs, discussed in Chapter 23, would extend to notifying an individual if his or her personal information might be transferred outside Australia.

Application of the 'Cross-border Data Flows' principle to agencies

31.152 The *Privacy Act* does not regulate the transfer of personal information outside Australia by agencies. Some state and territory privacy legislation contains a cross-border data flows principle that regulates the public sector in those jurisdictions,[233] and a number of overseas jurisdictions impose obligations concerning cross-border flows on both public and private sector bodies.[234]

31.153 The ALRC proposed, in DP 72, that the 'Cross-border Data Flows' principle should apply to agencies and organisations.[235] The vast majority of stakeholders supported this proposal.[236] For example, Medicare Australia submitted that individuals should be entitled to expect the same level of protection from agencies as from organisations.[237]

31.154 In the ALRC's view, the 'Cross Border Data Flows' principle should apply expressly to acts done, or practices engaged in, by agencies.

Recommendation 31–1 (a) The *Privacy Act* should be amended to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency.

---

232 Rec 31–9.

233 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPP 9; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 9; *Information Act 2002* (NT) sch 2, IPP 9.

234 See, eg, *Data Protection Act 1998* (UK) s 63 and *Federal Data Protection Act 1990* (Germany) ss 1, 2.

235 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–2.

236 Unisys, *Submission PR 569*, 12 February 2008; 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 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; Queensland Government, *Submission PR 490*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

237 Medicare Australia, *Submission PR 534*, 21 December 2007.

(b) The model Unified Privacy Principles should contain a principle called 'Cross-border Data Flows' that applies to agencies and organisations.

Transfers 'required or authorised by or under law'

31.155 A cross-border data flow principle that applies to agencies will need to provide for offshore transfers in certain circumstances.[238] The *Personal Information Protection Act 2004* (Tas), *Information Act 2002* (NT) and the Information Privacy Bill 2007 (WA)[239] provide that a state or territory agency may transfer information outside that jurisdiction if the transfer is 'required or authorised by or under law'.[240] The *Privacy Act 1985* (Canada) provides that Canadian governmental bodies may not disclose the personal data of individuals without their consent, subject to a number of exceptions, including disclosures made

> under an agreement or arrangement between the Government of Canada or an institution thereof and … the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation.[241]

Cross-border transfers of personal information required or authorised by federal Acts

Required by or under law

31.156 Some federal legislation imposes requirements on agencies and organisations to transfer personal information outside Australia in certain circumstances, for example, the:

- *National Health Security Act 2007* (Cth);[242] and
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act).[243]

Authorised by or under law

31.157 A number of federal Acts authorise cross-border transfers of personal information, for example, the:

---

238 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.
239 As at 5 May 2008, the Bill was before the Legislative Council.
240 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPP 9; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 9; *Information Act 2002* (NT) sch 2, IPP 9.
241 *Privacy Act* RS 1985, c P-21 (Canada) s 8(2)(f).
242 *National Health Security Act 2007* (Cth) ss 17, 27.
243 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 64(5).

- *National Health Security Act 2007* (Cth);[244]
- *Communications Legislation Amendment (Information Sharing and Datacasting) Act 2007* (Cth);[245]
- *Trade Practices Act 1974* (Cth);[246]
- *Australian Federal Police Act 1979* (Cth);[247] and
- AML/CTF Act.[248]

31.158 In addition, some legislation authorises disclosure for the purposes of international agreements or treaties, for example, the:

- *International Tax Agreements Act 1953* (Cth); [249] and
- *Social Security (Administration) Act 1999* (Cth).[250]

Discussion Paper proposal

31.159 In DP 72, the ALRC indicated that, should the 'Cross-border Data Flows' principle apply to agencies, an agency should not be liable for the transfer of personal information if it is necessary for law enforcement purposes. It noted that, in many cases, an agency will have no choice but to transfer information overseas, for example, for the purpose of a police investigation. The ALRC expressed the preliminary view that the law enforcement exception should not be worded as broadly as 'required or authorised by or under law'. The ALRC was concerned that such an exception might be too permissive in the context of transfer to overseas jurisdictions that may not have a similar level of privacy protection to Australia. It proposed, therefore, that the 'Cross-border Data Flows' principle should include a provision mirroring the law enforcement exception under the 'Use and Disclosure' principle (the 'law enforcement exception').[251]

Submissions and consultations

31.160 The general consensus of stakeholders was that the proposed 'law enforcement exception' was too narrow and that a 'required or authorised by or under' law

---

244 *National Health Security Act 2007* (Cth) ss 19(4), 27.
245 *Communications Legislation Amendment (Information Sharing and Datacasting) Act 2007* (Cth) s 59D.
246 *Trade Practices Act 1974* (Cth) s 155AAA(12).
247 *Australian Federal Police Act 1979* (Cth) s 60A.
248 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 132.
249 *International Tax Agreements Act 1953* (Cth) s 23.
250 *Social Security (Administration) Act 1999* (Cth) s 208(1)(b)(iii).
251 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–3. Note: in Proposal 28–3, the 'law enforcement exception' operated, in fact, as a condition on transfer under the 'Transborder Data Flows' principle proposed by the ALRC.

exception was both appropriate and warranted.[252] For example, the OPC submitted that 'legitimate agency transfers would be more appropriately dealt with by a "required or specifically authorised by or under law" provision'. In the OPC's view, such a condition would bring clarity and certainty to agencies whose enabling acts allow for disclosures and transfers overseas of personal information for particular purposes.[253] A large number of other agencies called for a 'required or authorised by or under law' exception. These included the following:

- the AFP, which called for an exception that allowed it to perform all of its functions under the *Australian Federal Police Act*—for example, disaster victim identification, the location of missing persons and provision of assistance to foreign law enforcement agencies for the purposes of enforcing foreign law—and expressed concern that such functions would not be caught by the proposed 'law enforcement exception';[254]

- ACMA, which expressed the view that the proposed 'law enforcement exception' may have the 'unintended consequence of impeding ACMA's statutory authority to disclose information relating to anti-spam activity to overseas agencies and organisations' under Part 7A of the *Broadcasting Services Act 1992* (Cth);[255]

- the Australian Taxation Office (ATO), which noted that it is obliged under various international treaties (made part of Australian domestic law under the *International Tax Agreements Act*) to provide information to overseas taxing authorities, if requested to do so by these agencies and submitted that its ability to honour those obligations should not be inhibited;[256]

- Centrelink, which indicated conditional support for the proposal on the basis that the 'Cross-border Data Flows' principle allowed the transfer of personal information outside Australia under obligations in the *Social Security (Administration) Act* that relate to international agreements;[257] and

---

252 Confidential, *Submission PR 570*, 13 February 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

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

254 Australian Federal Police, *Submission PR 545*, 24 December 2007.

255 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

256 Australian Taxation Office, *Submission PR 515*, 21 December 2007.

257 For example, s 208(1)(b)(iii) of the *Social Security (Administration) Act 1999* (Cth) allows for the disclosure of protected information to a competent authority or a competent institution of a foreign country that is party to a scheduled international social security agreement: Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

- the Department of Human Services, which called for an exception which would allow it to make disclosures necessary for compliance with an international treaty or other international agreement relating to maintenance obligations arising from family relationship, parentage or marriage, for example, under s 121B of the *Child Support (Registration and Collection) Act 1988* (Cth).[258]

31.161 The point also was made in a number of confidential submissions.[259] One stated:

> An exception for transfers by agencies where this is required or authorised by law should be included in the UPP to avoid any uncertainty where another law requires or authorises the transfer of information. … A broad authorised or required by law exception is preferable as there may also be other circumstances in which information is required to be transferred where not doing so may breach international obligations or requiring additional restrictions to be met may have real consequences in a timely response to a risk situation.[260]

31.162 In a similar vein, the ABA submitted that provision should be made in the UPPs for unconditional transborder data flows that are required by law.[261] This would cover the requirements on organisations to send personal information overseas in connection with international money transfers under the AML/CTF Act.

31.163 Some stakeholders supported the proposed 'law enforcement exception'.[262] There also was some qualified support.[263] For example, some submissions called for further elements to be added to the 'law enforcement exception'. One stakeholder argued that the exception needed to provide for the transfer of personal information in instances where there is a serious threat to life, health or safety.[264] The ACT Department of Disability, Housing and Community submitted that it may be useful to permit transfers where necessary to 'ensure the wellbeing and safety of the individual', noting that some children are placed overseas with their kin and their information is required to be transferred with them.[265] The Attorney-General's Department argued for the explicit inclusion of mutual assistance and extradition in the 'law enforcement

---

258 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

259 Confidential, *Submission PR 570*, 13 February 2008; Confidential, *Submission PR 448*, 11 December 2007.

260 Confidential, *Submission PR 570*, 13 February 2008.

261 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

262 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

263 Confidential, *Submission PR 570*, 13 February 2008; Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

264 Confidential, *Submission PR 570*, 13 February 2008.

265 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.

exception'.[266] The OPC disagreed, however, stating that 'disclosure and transfer overseas of information for extradition or mutual assistance purposes should be based on clear legislative authorisations'. [267]

31.164 Other stakeholders expressed the view that the proposed 'law enforcement exception' was too broad. Civil Liberties Australia argued that the proposal was inappropriately worded and would allow for broadbrush transmission of information. It proposed instead that an agency or organisation should be permitted to transfer data across borders 'if empowered to do so under legislation or regulations applying to them', but submitted that where such transfers took place, Australian privacy principles, requirements and penalties should attach to the transferred data and its use by the transferee. It argued that this was no different from the transfer of guarantees or warranties in the manufacturing and retail sector.[268]

31.165 Some stakeholders called for a requirement that agencies and organisations seek assurances about privacy protection in relation to such transfers. The Australian Privacy Foundation and the Cyberspace Law and Policy Centre were reluctant to support the proposed 'law enforcement exception', unless it was more tightly worded. They expressed concern that the proposal would allow for the transfer of personal information to a wide range of bodies in jurisdictions 'not only lacking in privacy protection rules, but also lacking in basic standards of legitimacy, human rights or natural justice'. They argued that, at the very least, agencies and organisations transferring under the proposed law enforcement exception should be required to seek assurances about privacy protection.[269]

31.166 The OPC submitted that where an agency proposed to transfer personal information for law enforcement, extradition and mutual assistance purposes to a country without privacy protections similar to the UPPs, agencies should establish administrative arrangements or MOUs or protocols regarding appropriate handling practices for such information.[270] ACMA noted that it has MOUs in place with various overseas regulatory organisations, which broadly set out mutually agreed arrangements for the reciprocal exchange of information. Signatories to these MOUs include government regulators and law enforcement agencies.[271]

31.167 Some stakeholders addressed the relationship between the proposed law enforcement exception and the 'Use and Disclosure' principle. The Australian Privacy Foundation and the Cyberspace Law and Policy Centre noted that the exceptions to the 'Cross-border Data Flows' principle are an additional hurdle than must be crossed

---

266 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
267 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
268 Civil Liberties Australia, *Submission PR 469*, 14 December 2007.
269 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
270 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
271 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

where an overseas transfer is involved. That is, the transfer also will need to comply with the 'Use and Disclosure' principle. Given this relationship, they questioned why the law enforcement exception needed to replicate some of the law enforcement exceptions in the 'Use and Disclosure' principle.[272]

31.168 Some stakeholders argued that the proposed 'law enforcement exception' should be limited to Australian agencies or Australian laws. The OPC's proposal was predicated on 'law' being limited to Australian laws, consistent with the approach taken in the *Acts Interpretation Act 1901* (Cth). The OPC also expressed the view that overseas law enforcement requests for personal information should be mediated by Australian law enforcement agencies. Its view was that overseas law or other matter should not be relied upon to authorise the disclosure of personal information.[273] PIAC agreed that there should be an exception, but argued it should apply only to Australian enforcement bodies.[274]

31.169 ACMA expressed concern that the proposed 'law enforcement exception' was too narrow in its application—that is, it needed to apply to bodies other than law enforcement bodies. It submitted that the use of the words

> 'by or on behalf of an enforcement body' may have the effect, for some overseas jurisdictions, of restricting ACMA's ability to share information with the appropriate overseas government organisation charged with anti-spam minimisation or enforcement …
>
> A broader exception should be adopted to ensure that 'Australian' law enforcement and regulatory authorities are not prevented from making disclosures to coregulators and enforcement bodies which may not fall within the meaning of 'enforcement body'.[275]

ALRC's view

31.170 Under the 'Cross-border Data Flows' principle, one of the circumstances in which the default position of accountability will not apply is where an agency or organisation is 'required or authorised by or under law' to transfer the personal information to a recipient outside of Australia. In making this recommendation, the ALRC acknowledges the view expressed by many stakeholders that such an exception would facilitate more appropriately legitimate agency transfers than one limited to 'law enforcement' purposes. Strong concerns were expressed by agencies that the 'law enforcement exception' in DP 72 may have had the unintended consequence of impeding their ability to make disclosures necessary to the fulfilment of their statutory functions.

---

272 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

274 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

275 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

31.171 International transfer of personal information by agencies should be based on legislative requirements or authorisations, although such authorisations may be implied. As discussed in Chapter 16, the ALRC recommends that the term 'law', for the purposes of the 'required or authorised by or under law' exception, be defined to include federal, state and territory Acts and delegated legislation.[276] It should not include the legislation of a foreign country.

31.172 To confine the application of the exception to law enforcement bodies is too narrow in that it may not allow, for example, cross-border transfers required to manage risks to public health[277] or to address the problem of spam.[278] There are situations in which an organisation may be required by law to execute a cross-border transfer of personal information.[279] The 'required or authorised by or under law' exception should apply both to agencies and organisations.

31.173 The ALRC encourages the establishment, by agencies, of administrative arrangements, MOUs or protocols regarding appropriate personal information-handling practices with countries without privacy protection similar to the UPPs in place. The OPC should provide guidance in relation to the establishment of those arrangements.

Terminology

31.174 NPP 9 currently regulates when an organisation may transfer personal information about an individual to 'someone' who is in a 'foreign country'.

31.175 In DP 72, the ALRC proposed that the 'Cross-border Data Flows' principle should refer to the transfer of personal information to a 'recipient' rather than 'someone', in order to make it clear that the principle applies to the overseas transfer of personal information to agencies, organisations and individuals.[280] Also, the ALRC proposed that NPP 9 be amended to refer to 'outside Australia' rather than to a 'foreign country', as it suggested a broader reading of what an overseas jurisdiction may be. Further, it was consistent with language in overseas and state and territory cross-border data principles.[281] The ABA and the Cyberspace Law and Policy Centre supported the suggested change in terminology.[282] The ALRC's proposed terminology is confirmed in the recommendation below.

---

276 Rec 16–1.

277 For example, the *National Health Security Act 2007* (Cth) s 19 provides for the sharing of information with the World Health Organisation and countries affected by an event relating to public health or an overseas mass casualty.

278 See Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

279 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 64(5).

280 Stakeholder views on these issues were discussed in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.42]–[28.44].

281 *Personal Data (Privacy) Ordinance* (Hong Kong) s 33(1); *Privacy and Personal Information Protection Act 1998* (NSW) s 19(2); *Information Privacy Act 2000* (Vic) sch 1, IPP 9; *Personal Information Protection Act 2004* (Tas) sch 2, PIPP 9; *Information Act 2002* (NT) sch 2, IPP 9.

282 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

31.176 In DP 72, UPP 11 was called the 'Transborder Data Flow' principle, picking up on the terminology used currently in NPP 9. The ALRC recommends that the principle be called the 'Cross-border Data Flows' principle, in order to ensure consistency with the terminology commonly used, such as in the APEC Privacy Framework.[283]

Recommendation 31–2 The 'Cross-border Data Flows' principle should provide that, if an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia or an external territory, the agency or organisation remains accountable for that personal information, unless the:

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model Unified Privacy Principles;

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

(c) agency or organisation is required or authorised by or under law to transfer the personal information.

Recommendation 31–3 The *Privacy Act* should be amended to provide that 'accountable', for the purposes of the 'Cross-border Data Flows' principle, means that where an agency or organisation transfers personal information to a recipient (other than the agency, organisation or the individual) that is outside Australia or an external territory:

(a) the recipient does an act or engages in a practice outside Australia or an external territory that would have been an interference with the privacy of the individual if done or engaged in within Australia or an external territory; and

(b) the act or practice is an interference with the privacy of the individual, and will be taken to have been an act or practice of the agency or organisation.

283 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [44]–[46].

Interaction with the 'Use and Disclosure' principle

31.177 Under the NPPs, an organisation that wants to transfer personal information outside Australia needs to determine whether the disclosure of that information to someone outside Australia will comply with NPP 2 (the Use and Disclosure principle). The organisation then needs to determine whether the transfer will satisfy at least one of the conditions set out under NPP 9. This should continue to be the case under the proposed UPPs in relation to both agencies and organisations.

31.178 In DP 72, the ALRC proposed that both the 'Use and Disclosure' principle and the 'Cross-border Data Flows' principle should include notes cross-referencing to the other, in relation to cross-border transfers of personal information.[284]

31.179 The majority of stakeholders supported this proposal.[285] The OPC noted that it would assist in clarifying obligations for agencies and organisations.[286] The Australian Privacy Foundation and the Cyberspace Law and Policy Centre noted that the relationship and interaction between the 'Use and Disclosure' and the 'Cross-border Data Flows' principles needed to be explained more clearly.[287]

31.180 Privacy NSW submitted that the proposal involved circularity, in the sense that each principle referred to the other in defining its scope. It submitted that the 'Cross-border Data Flows' principle should be called the 'Disclosure to Other Countries' thereby obviating the need for 'circular considerations'.[288]

31.181 It is preferable that all disclosures of personal information be regulated by the 'Use and Disclosure' principle—this allows for consistent treatment of all personal information. The 'Cross-border Data Flows' principle is concerned only with the cross-border transfer of that personal information. For this reason, there is no circularity. The notes in the 'Use and Disclosure' principle and the 'Cross-border Data Flows' principle, cross-referencing to the other in relation to cross-border transfers of personal information, provide greater clarity about the interaction between the two principles.

---

284 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 28–5, 28–6.

285 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 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; Queensland Government, *Submission PR 490*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

287 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

288 Privacy NSW, *Submission PR 468*, 14 December 2007.

Recommendation 31–4 A note should be inserted after the:

(a) 'Use and Disclosure' principle, cross-referencing to the 'Cross-border Data Flows' principle; and

(b) 'Cross-border Data Flows' principle, cross-referencing to the 'Use and Disclosure' principle.

Definition of 'transfer'

31.182 The ALRC also examined whether it would be useful to distinguish the term 'transfer' from the terms 'use' and 'disclosure'. One option for dealing with this issue is to define 'transfer' in the *Privacy Act* to include the situation where personal information is stored in Australia in such a way that allows it to be accessed and viewed outside Australia. This definition clearly would capture the transfer of personal information on intranets and password-protected sections of websites. It also would include uploading personal information on the internet.

31.183 Another issue arises when an agency or organisation sends an email containing personal information by or to email systems that are hosted overseas.

> Imagine, for example, a situation where an Australia doctor emails some test results to an Australian patient. Imagine further that the patient is using Microsoft's Hotmail system. While the e-mail is sent from one Australian party to another, the e-mail including the sensitive personal information it contains, may be stored on a server overseas. Has the Australian doctor in this situation transferred personal information to someone in a foreign country? The answer would seem to be yes, as the information is placed on a server located in a foreign country.[289]

31.184 In DP 72, the ALRC asked whether the *Privacy Act* should provide that, for the purposes of the proposed 'Cross-border Data Flows' principle, a 'transfer':

- includes where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia; and

- excludes the temporary transfer of personal information, such as when information is emailed from one person located in Australia to another person also located in Australia, but, because of internet routing, the email travels

289 D Svantesson, 'Protecting Privacy on the "Borderless" Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168, 184.

(without being viewed) outside Australia on the way to its recipient in Australia?[290]

Submissions and consultations

31.185 A wide range of views were received on this question. Some stakeholders agreed with the ALRC's proposed definition of the term 'transfer'.[291]

31.186 Others expressed more qualified agreement. In the OPC's view, the term 'transfer' should be defined, but it 'should not exclude information transferred overseas accidentally because the sending entity has not taken reasonable steps to protect the personal information'.[292]

31.187 Other stakeholders disagreed. Microsoft noted that the difficulties associated with defining the concept of 'transfer' provided another justification for adopting the APEC accountability model, which does not turn on this concept. It argued that such concepts would become only more 'difficult to define as emerging technologies further blur the question of where records are stored and the distinction between permanent and temporary copies of electronic records'.[293]

Personal information stored in Australia but accessed or viewed outside Australia

31.188 There was no consensus from stakeholders as to whether the term 'transfer' should include circumstances in which personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia. A number of stakeholders supported its inclusion.[294] Others, such as GE Money, argued that a 'transfer would not occur merely because it was possible for the information to be accessed or viewed outside of Australia, but only if this actually occurs'.[295] This point also was made by another stakeholder, who submitted:

> This is appropriate because many organisations which operate internationally have servers which can be accessed from multiple jurisdictions. It is not appropriate to require that consent be obtained from an individual (or that another exception be triggered) merely to include an individual on a database with such a facility. The point

290 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 28–1. The impact of the internet on privacy is discussed in Chs 9 and 11.

291 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

293 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

294 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

295 GE Money Australia, *Submission PR 537*, 21 December 2007.

> at which any consent should be required is the point at which access is actually given to a particular record.[296]

31.189 There also were stakeholders who opposed the inclusion of this in the definition.[297] In the ABA's view, the way in which it would operate in practice, and its effect on a bank's operations, were uncertain.[298]

Excluding temporary transfer of information

31.190 Again, there was a lack of consensus about whether a definition of transfer should exclude the temporary transfer of personal information, such as when information is emailed from one person located in Australia to another person also located in Australia, but, because of internet routing, the email travels (without being viewed) outside Australia on the way to its recipient in Australia. Some stakeholders supported its exclusion.[299] In Microsoft's view, such transfers 'should fall outside the scope of regulation, because the compliance costs associated with regulating these types of transfers would far outweigh the privacy gain to the individual'.[300] Google submitted that the definition needed to be broader, covering situations where the sender is in Australia and the recipient is outside Australia, and where reliance is placed upon, for example, consent.[301]

31.191 The OVPC submitted that there should be some provision for online transactions, which also often involve extensive and instantaneous transborder transfers of data.[302] In the view of the Cyberspace Law and Policy Centre, the communication of data by routes which enable it to be intercepted by parties outside Australia should constitute a transfer. It submitted:

> A 'transfer' should only occur if there is a recipient outside Australia who uses or stores the information for purposes other than communicating it to final recipient. Communications may involve temporary storage, but if the information is subject to set retention periods whether required by law or otherwise, there will be a transfer.[303]

ALRC's view

31.192 There is a high level of complexity attaching to the way in which personal information is transferred. Also, as noted above, a wide range of views was received from stakeholders on this question. Generally, if personal information is stored in

---

296 Confidential, *Submission PR 536*, 21 December 2007.

297 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

298 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

299 Ibid; GE Money Australia, *Submission PR 537*, 21 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

300 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

301 Google Australia, *Submission PR 539*, 21 December 2007.

302 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

303 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

Australia, but is accessed or viewed outside Australia, it should be considered to have been transferred. If personal information is routed and temporarily stored outside Australia, but is not accessed, it should not fall within the purview of the 'Cross-border Data Flows' principle. If it is accessed, however, it should be subject to the principle.

31.193 That said, providing a definition of 'transfer' in the *Privacy Act* is unlikely to clarify the situation, given rapid advances in technology and the difficulty of the distinction between the temporary and permanent storage of information. The term 'transfer' should not be defined for the purposes of the *Privacy Act.* It is preferable to resolve the question on a case-by-case basis, with the assistance of OPC Guidance.

31.194 The OPC Guidance relating to cross-border data flows should provide examples of circumstances in which a transfer would, or would not, be taken to have occurred for the purposes of the 'Cross-border Data Flows' principle.[304] Such guidance can more readily be amended to accommodate changes to the ways in which personal information is transferred than a definition of 'transfer' under the *Privacy Act*.

Related bodies corporate

31.195 NPP 9 does not prevent transfers of personal information outside Australia by an organisation to another part of the same organisation, or to the individual concerned.[305] As noted above, the *Privacy Act* operates extraterritorially in these circumstances by virtue of s 5B.

31.196 A company transferring personal information overseas to another related company, however, must comply with NPP 9. Section 13B(1) states that an act or practice is not an interference with the privacy of an individual if it involves a body corporate collecting or disclosing personal information (that is not sensitive information) from or to a related body corporate. A 'related body corporate' is a body corporate that is: a holding company of another body corporate; a subsidiary of another body corporate; or a subsidiary of a holding company of another body corporate; and the first mentioned body and the other body are related to each other.[306]

31.197 In submissions to the OPC Review, a number of stakeholders called for clarification of the interaction between NPP 9 and s 13B(1). They argued that it was unclear whether s 13B(1) made it possible for a body corporate in Australia to transfer personal information to a related body corporate located outside Australia without reference to NPP 9.[307]

---

304 Rec 31–7.

305 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58.

306 This definition is from the *Corporations Act 2001* (Cth) s 50, as referred to in s 6(8) of the *Privacy Act 1988* (Cth). For a general discussion of the exemption, see Ch 43.

307 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 77.

31.198 The OPC Review concluded that, where information is transferred outside of Australia and the extraterritorial provisions do not apply, it is in the public interest for NPP 9 to apply. The OPC, therefore, did not recommend excluding related corporations from having to comply with NPP 9.[308]

31.199 In DP 72, the ALRC proposed that s 13B of the *Privacy Act* be amended to clarify that, if an organisation transferred personal information to a related body corporate outside Australia, that transfer would be subject to the proposed 'Cross-border Data Flows' principle.[309]

Submissions and consultations

31.200 Many stakeholders supported the proposal.[310] There also were some stakeholders who disagreed. For example, one stakeholder submitted:

> In practice, the main effect of imposition of the cross-border data flows rules within company groups is likely to impose an unnecessary layer of red tape and bureaucracy. For example, many company groups would be likely to respond simply by having all companies in the group sign a contract agreeing to comply with the UPPs.[311]

31.201 Microsoft submitted that the ALRC should consider the introduction of an exemption for related bodies corporate that operate under a common set of internal policies, which would provide for at least the same level of protection as the *Privacy Act*. In Microsoft's view, such an approach would be consistent with the commitment of APEC members to support the development and recognition of CBPRs across APEC.[312]

31.202 Similarly, GE Money was concerned that the proposal did not 'consider the issues presented for organisations that form part of a large multinational company'. It argued that the proposal, when combined with the impact of proposals relating to the removal of the employee records exemption, had the potential to impede the collection and recording of employee information in an accurate and efficient way.[313]

---

308 Ibid, 79.

309 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–7.

310 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007l; Optus, *Submission PR 532*, 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; Queensland Government, *Submission PR 490*, 19 December 2007.

311 Confidential, *Submission PR 536*, 21 December 2007. See also ANZ, *Submission PR 467*, 13 December 2007.

312 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

313 GE Money Australia, *Submission PR 537*, 21 December 2007.

ALRC's view

31.203 If personal information is sent overseas to the same company, it will continue to be protected by the *Privacy Act* because the extraterritorial provisions apply. Section 5B, however, does not apply to related bodies corporate outside of Australia. As such, if personal information is sent to a related company, it may not be protected by the *Privacy Act*.

31.204 Although many related companies are governed by a common set of internal policies, this may not always be the case. Further, the internal policies of a related company may not always provide the same level of protection as the *Privacy Act*.

31.205 Where information is transferred outside of Australia by an organisation to a related body corporate, it is in the public interest for the 'Cross-border Data Flows' principle to apply.

Recommendation 31–5 Section 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia or an external territory, the transfer will be subject to the 'Cross-border Data Flows' principle.

List of overseas jurisdictions

31.206 The *Privacy Act* does not provide a definition of what constitutes a 'substantially similar' set of principles for the purposes of NPP 9(a).[314] The OPC Review noted that stakeholders had expressed frustration at the lack of guidance regarding the countries whose laws provide adequate protection equivalent to the NPPs.

> In this situation the onus is on the organisation to assess the regime of the country in which their trading partner resides. Many stakeholders, especially small businesses, have criticised the efficiency of this system arguing that they neither have the expertise or the resources to assess a foreign country's privacy laws.[315]

31.207 In the context of the OPC Review, it was suggested that the OPC could publish a list of countries with substantially similar privacy laws. The OPC rejected this proposal on the basis that it was a complex task that would require considerable resources. The OPC also suggested that such a task could affect its relationships with other countries and may be an inappropriate task for it to undertake.[316]

---

314 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [2-5800].

315 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

316 Ibid, 79.

31.208 In its submission to the House of Representatives Committee on Legal and Constitutional Affairs inquiry into the Privacy Amendment (Private Sector) Bill 2000 (Cth), the European Commission argued that 'it is our experience that it is difficult for the average operator to have substantial knowledge of the level of protection of personal data in third countries'.[317]

31.209 In IP 31, the ALRC asked what role, if any, the OPC should play in identifying countries that have protection for personal information equivalent to the *Privacy Act*.[318] In DP 72, the ALRC acknowledged that such a role would have considerable resource implications. The ALRC proposed, therefore, that the Australian Government develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the UPPs.[319]

Submissions and consultations

31.210 Most stakeholders who commented on this proposal expressed their support.[320] Submissions noted that the list would assist individuals to make choices about the handling of personal information, and businesses to make decisions about when alternative arrangements are needed to protect personal information.[321] The Association of Market and Social Research Organisations and the Australian Market and Social Research Society submitted that the difficulty in determining the equivalence of other countries' privacy regimes with Australia's has created additional unnecessary barriers for Australian organisations wishing to trade overseas. In their view, knowing which countries guarantee substantially similar privacy rights for individuals is essential, but can be difficult for organisations to ascertain. They submitted that the OPC should be involved.[322]

---

317 European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (2000), 7.

318 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–3. The submissions on this issue are canvassed in detail in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.89]–[28.91].

319 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–8.

320 Unisys, *Submission PR 569*, 12 February 2008; Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

321 Unisys, *Submission PR 569*, 12 February 2008; Australian Collectors Association, *Submission PR 505*, 20 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

322 Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007.

31.211 In the OPC's view, however, the task of interpreting and assessing a large number of different privacy laws and legal systems would not be an appropriate role for the OPC. The OPC submitted that these types of decisions were best left to governments, acting with the advice of privacy commissioners.[323] PIAC agreed that the OPC should not have responsibility for developing the list, but submitted that, along with privacy advocates and consumer groups, it should have input.[324]

31.212 Some support for the proposal was qualified. IBM Australia Ltd, while welcoming the proposal, submitted that 'the proposed list should not be the definitive requirement for determining whether an organisation is complying' with the relevant privacy principle when transferring information overseas.[325]

31.213 The Australasian Compliance Institute supported the proposal as an initial mechanism to determine 'jurisdictional compatibility' and submitted that the list should be updated and maintained on an ongoing basis.[326] The National Australia Bank submitted that reliance on the list should constitute 'reasonable belief' for the purposes of the 'Cross-border Data Flows' principle.[327]

31.214 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre submitted that there should be a 'whitelist' of countries with equivalent laws, promulgated as a regulation or other legislative instrument made by the government, after receipt of published advice by the Privacy Commissioner.[328] The Australian Privacy Foundation submitted that it is unrealistic to assume that, where an overseas scheme upholds privacy protections effectively, an individual can seek redress overseas. To address this concern, it suggested:

> In order to qualify for the 'whitelist' for the purposes of UPP11(a), a foreign jurisdiction must have in place an agreement on cross border enforcement with the OPC.
>
> Except where a transfer is to a jurisdiction included in a 'whitelist' legislative instrument, the agency or organisation should continue to be liable for any breaches of the UPPs …[329]

31.215 The Cyberspace Law and Policy Centre submitted that there was little point in 'pretending' that such a whitelist would not automatically qualify as a basis for

---

323 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. In expressing this view, the OPC was agreeing with the view expressed by the OVPC in its submission to IP 31: Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

324 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

325 IBM Australia, *Submission PR 405*, 7 December 2007. See also Australian Information Industry Association, *Submission PR 410*, 7 December 2007.

326 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007. See also National Australia Bank, *Submission PR 408*, 7 December 2007.

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

328 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

329 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. See also Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

'reasonable belief' under the 'Cross-border Data Flows' principle, so this should be made explicit in the relevant regulations.[330]

ALRC's view

31.216 The benefits of developing a list of laws and binding schemes that have equivalent *Privacy Act* protection for personal information far outweigh any disadvantages. Stakeholders have identified clearly the need for a list on a number of occasions, including in submissions to this Inquiry.[331] Such a list would assist agencies and organisations to comply with the proposed 'Cross-border Data Flows' principle. Further, it would assist individuals to make choices based on where their personal information may be transferred, and how it will be handled.

31.217 The ALRC accepts that this task would have considerable resource implications for the OPC. The ALRC therefore recommends that the Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the model UPPs. This may be a suitable task for the Department of Prime Minister and Cabinet,[332] in consultation with other Australian Government agencies, such as DFAT and the OPC.[333]

31.218 While inclusion on the list is a good basis for 'reasonable belief' for the purposes of the 'Cross-border Data Flows' principle, the list should not be enacted as a legislative instrument. If the list is maintained more informally, it is able to be updated easily and frequently. The list will be more useful if current. Also, as discussed above, the question of whether the test in (a) of the 'Cross-border Data Flows' principle is satisfied should be resolved on a case-by-case basis.

Recommendation 31–6 The Australian Government should develop and publish a list of laws and binding schemes in force outside Australia that effectively uphold principles for the fair handling of personal information that are substantially similar to the model Unified Privacy Principles.

---

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

331 See also European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (2000); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

332 Responsibility for the *Privacy Act* falls under the Department of the Prime Minister and Cabinet: Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

333 The ALRC notes that Ernst & Young has compiled such a list: Ernst & Young, *Data Protection in the European Union and Other Selected Countries: A New Comparative Study* (2006).

Cross-border enforcement

31.219 The ability to investigate breaches of local privacy laws in foreign countries poses particular challenges for privacy regulators.[334] The OECD identified considerable scope for a more global and systematic approach to cross-border privacy law enforcement cooperation.[335]

31.220 The ALRC notes that the OPC is already involved in a number of forums aimed at improving cooperative arrangements between privacy regulators in other jurisdictions. For example, the OPC is a member of the Asia Pacific Privacy Authorities (APPA) Forum. APPA meets biannually and includes the federal, state and territory privacy regulators of Australia, New Zealand, Hong Kong and South Korea. APPA's objectives include: facilitating the sharing of knowledge and resources between privacy authorities within the region; fostering cooperation in privacy and data protection; promoting best practice amongst privacy authorities; and working to improve performance to achieve the objectives set out in privacy laws of each jurisdiction.[336]

31.221 In addition, as discussed above, the Australian Government, including the OPC, is involved in the implementation of the APEC Privacy Framework and is leading three of the Data Pathfinder Projects.[337] This will involve cooperation between regulators in APEC economies.[338]

31.222 The OPC also has entered into an agreement with the New Zealand Privacy Commissioner that allows for cooperation on privacy related issues. The MOU covers the sharing of information related to surveys, research projects, promotional campaigns, education and training programs, and techniques in investigating privacy violations and regulatory strategies. Other areas addressed include cooperation on complaints with a cross-border element and the possible undertaking of joint investigations. The ALRC encourages the Australian Government and the OPC to continue to seek opportunities for further cooperation with privacy regulators outside Australia. This will be important to the effective implementation of the recommended 'Cross-border Data Flows' principle.

---

334 See, eg, *Lawson v Accusearch Inc* (2007) (Federal Court of Canada, Harrington J, 5 February 2007).

335 Organisation for Economic Co-operation and Development, *Report on the Cross-Border Enforcement of Privacy Laws* (2006), 4.

336 Asia Pacific Privacy Authorities Forum, *Statement of Objectives* (2005).

337 K Curtis, 'Information Workshop for Australian Stakeholders' (Paper presented at APEC Data Privacy Pathfinder Seminar, Sydney, 6 February 2008), 5–7.

338 See, eg, *Second Technical Assistance Seminar on the International Implementation of the APEC Privacy Framework*, Cairns, 25–26 June 2007.

OPC Guidance

Contractual arrangements

31.223 NPP 9 and the recommended 'Cross-border Data Flows' principle anticipate that organisations will use contracts to protect personal information when it is transferred outside Australia.

31.224 The OPC Review noted that:

> From submissions and the comments received during stakeholder workshops, it appears that organisations are fulfilling their NPP 9 obligations of ensuring that personal information is protected when it is transferred to regions without privacy regimes through contractual arrangements with their trading partners. While some submissions find this to be an effective solution, others are concerned about the costs associated with monitoring the compliance of their trading partners.[339]

31.225 The OPC Review noted that the OPC could provide greater guidance by publishing approved standard contractual provisions for use by Australian companies and international trading partners. It indicated that the EU had issued contract provisions. It acknowledged, however, that developing standard contractual provisions would have resource implications for the Office.[340] Rather than publishing standard contractual provisions, the OPC recommended that it provide further guidance to assist organisations in complying with NPP 9.[341]

31.226 In DP 72, the ALRC proposed that the OPC issue guidance on the issues that should be addressed as part of a contractual agreement with the overseas recipient of personal information.[342] PIAC submitted that it would be helpful if the OPC guidance provided model contractual provisions as the OVPC has done.[343]

Other OPC guidance

31.227 In other sections of this chapter, the ALRC proposes that guidance on the proposed 'Cross-border Data Flows' principle also should address:

- when personal information may become available to a foreign government;
- contracting out government services to organisations outside Australia;

---

339 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

340 Ibid, 78.

341 Ibid, Rec 18.

342 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–9(c).

343 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also: Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007.

- what constitutes a 'reasonable belief';

- consent to cross-border data flows, including information for individuals on the consequences of providing consent;

- the establishment by agencies of administrative arrangements or MOUs or protocols with foreign governments, with respect to appropriate handling practices for personal information in overseas jurisdictions where privacy protections are not substantially similar to the model UPPs (for example, where the transfer is required or authorised by or under law); and

- examples of the circumstances in which a transfer will, and will not, be taken to have occurred, for the purposes of the 'Cross-border Data Flows' principle.[344]

31.228 The majority of stakeholders supported the ALRC's proposals in relation to OPC guidance.[345] Medicare Australia's support for the model 'Cross-border Data Flows' principle was conditional on OPC guidance being made available, to ensure consistent interpretation and application of specific criteria.[346] On the other hand, GE Money expressed concern at the extent of guidance recommended by the ALRC.[347]

31.229 The OPC agreed that it should develop general guidance for agencies and organisations regarding the risks of personal information being made available to foreign governments. That guidance should include a warning that foreign laws might require the disclosure of the information to foreign government agencies and general advice about minimising privacy risks when transferring personal information overseas.[348] The OVPC submitted that guidance should be produced jointly, or in consultation with, state or territory privacy commissioners.[349]

ALRC's view

31.230 The OPC should develop and publish guidance about the issues that should be addressed as part of a contractual agreement with the overseas recipient of personal

---

344 In Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 28–9, the ALRC proposed that the OPC issue guidance in relation to some elements of NPP 9 that have been removed from the recommended 'Cross-border Data Flows' principle. Guidance, therefore, is not required in relation to those matters (specifically, items (d) and (e) of Proposal 28–9).

345 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; 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; Optus, *Submission PR 532*, 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; Queensland Government, *Submission PR 490*, 19 December 2007.

346 Medicare Australia, *Submission PR 534*, 21 December 2007.

347 GE Money Australia, *Submission PR 537*, 21 December 2007.

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

349 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

information. This guidance will be particularly helpful for small businesses. The ALRC notes that the OVPC has published *Model Terms for Cross-border Data Flows of Personal Information*. The guide includes model clauses for the transfer of personal information outside Victoria, together with commentary about the clauses.[350] In the ALRC's view, the OPC should provide model clauses as part of that guidance.

31.231 Further, OPC guidance in the areas discussed above would assist agencies and organisations to comply with the 'Cross-border Data Flows' principle.

Recommendation 31–7 The Office of the Privacy Commissioner should develop and publish guidance on the 'Cross-border Data Flows' principle, including guidance on:

(a) circumstances in which personal information may become available to a foreign government;

(b) outsourcing government services to organisations outside Australia;

(c) the issues that should be addressed as part of a contractual agreement with an overseas recipient of personal information;

(d) what constitutes a 'reasonable belief';

(e) consent to cross-border data flows, including information for individuals on the consequences of providing consent;

(f) the establishment by agencies of administrative arrangements, memorandums of understanding or protocols with foreign governments, with respect to appropriate handling practices for personal information in overseas jurisdictions where privacy protections are not substantially similar to the model Unified Privacy Principles (for example, where the transfer is required or authorised by or under law); and

(g) examples of circumstances which do, and do not, constitute a transfer for the purposes of the 'Cross-border Data Flows' principle.

350 Office of the Victorian Privacy Commissioner, *Model Terms for Cross-border Data Flows of Personal Information* (2006).

Requirement of notice that personal information is being sent overseas

31.232 As noted above, a large number of respondents to the ALRC's National Privacy Phone-In expressed concerns about Australian companies sending their personal information overseas.[351]

31.233 In IP 31, the ALRC asked whether organisations should be required to inform individuals that their personal information is to be transferred outside Australia, and if so, what form such notification should take.[352] Most stakeholders submitted that individuals should be informed that their personal information is to be transferred outside Australia.[353] The form in which the notice is given is relevant to the compliance burden placed on agencies and organisations. There is an enormous cost difference depending on whether notice has to be given to each individual or whether it could be posted, for example, on a company's website. It was noted that, for large companies, the cost of complying with the requirement to give notice could run to millions of dollars.

31.234 In DP 72, the ALRC stated that, if personal information will or may be transferred outside Australia, agencies or organisations should be required to notify individuals, but that it would be too onerous to require notification with respect to each transfer. The ALRC proposed that the Privacy Policy of an agency or organisation, referred to in the proposed 'Openness' principle, should set out whether personal information may be transferred outside Australia.[354]

Submissions and consultations

31.235 Many stakeholders supported the ALRC's proposal.[355] The OPC submitted that a Privacy Policy should set out whether the personal information is 'likely' to be transferred outside Australia.[356] PIAC expressed the view that the policy should also specify the countries to which personal information may be transferred.[357]

---

351 *National Privacy Phone-In*, June 2006.

352 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–4.

353 Stakeholder views on this issue are set out in detail in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [28.112]–[28.117].

354 Ibid, Proposal 28–10.

355 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; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 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; Queensland Government, *Submission PR 490*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007.

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

357 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

31.236 The Australian Privacy Foundation also expressed its support for the proposal, indicating that 'a requirement to notify would be one of the most effective protections against inappropriate transfers'. It submitted that the requirement should include notification of which jurisdiction the information would be transferred to and the identity of the recipient in that jurisdiction, so as to assist individuals to make an 'informed choice' about their personal information or 'bring pressure to bear for improvements in legislative protection'. In its view, specific notification should be made a condition of the consent exception in the 'Cross-border Data Flows' principle.[358]

31.237 ANZ was supportive of notifying customers, through a Privacy Policy, of the transfer of personal information overseas. The policy could outline the circumstances in which personal information is sent overseas and the types of information security controls that have been implemented to protect that information.[359]

31.238 GE Money opposed the ALRC's proposal, on the basis that a Privacy Policy needs to be a 'high level and relatively brief document'.

> There may be many different divisions or businesses of an organisation that have different information-handling needs and practices. For some organisations privacy information is provided to customers and clients that is business or product specific. It should be open to an organisation to include this information in these sorts of privacy notices and consent forms (where they are provided) and not have to also include this information in a privacy policy where it may not be possible to be accurate about the specific situations where information will and will not be transferred outside of Australia.[360]

ALRC's view

31.239 If personal information will, or may, be transferred outside Australia, agencies and organisations should be required to notify individuals. This would help individuals to exercise informed choice about how their personal information will be dealt with, and the level of privacy protection it will receive. Requiring notification or written consent each time an agency or organisation transfers an individual's personal information overseas, however, would result in an unjustified compliance burden.

31.240 The 'Notification' principle will require an agency or organisation that collects personal information about an individual from the individual, to take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of a number of matters, including actual or types of organisations, agencies, entities or other persons to whom the agency or organisation

---

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

359 ANZ, *Submission PR 467*, 13 December 2007.

360 GE Money Australia, *Submission PR 537*, 21 December 2007.

usually discloses personal information.[361] The requirement would extend to notifying an individual if his or her personal information might be transferred outside Australia. The description of an agency or organisation provided as part of that notification may alert an individual to the country or countries to which his or her information is likely to be transferred.

31.241 Further, the ALRC recommends, in Chapter 24, that the 'Openness' principle should require agencies and organisations to create a Privacy Policy that sets out their policies on the management of personal information.[362] This Privacy Policy should set out whether personal information may be transferred outside Australia and the countries to which information is likely to be transferred. If the policy of an agency or organisation changes on transfer of personal information outside Australia, the Privacy Policy should be updated to reflect this.

Recommendation 31–8 The Privacy Policy of an agency or organisation, referred to in the 'Openness' principle, should set out whether personal information may be transferred outside Australia and the countries to which such information is likely to be transferred.

Summary of 'Cross-border Data Flows' principle

31.242 The eleventh principle in the model UPPs should be called 'Cross-border Data Flows'. It may be summarised as follows.

UPP 11. Cross-border Data Flows

11.1 If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;

361 Rec 23–2. The 'Notification' principle, discussed in detail in Ch 23, was referred to as the 'Specific Notification' principle in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007).

362 Rec 24–1.

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

(c) agency or organisation is required or authorised by or under law to transfer the personal information.

Note: Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

32. Additional Privacy Principles

Contents

Introduction

32.1 In this chapter, the ALRC considers whether the model Unified Privacy Principles (UPPs) should cover aspects of privacy that are not currently covered by the Information Privacy Principles (IPPs) or National Privacy Principles (NPPs).[1] In particular, the ALRC assesses the potential benefits of:

- an 'Accountability' principle;
- a 'Prevention of Harm' principle; and
- a 'No Disadvantage' principle.

32.2 In other chapters in this Report, the ALRC considers potential new privacy principles dealing with consent[2] and data breach notification.[3]

---

1 The ALRC recommends that the IPPs and NPPs should be consolidated into a single set of privacy principles, the UPPs, which would be generally applicable to agencies and organisations: see Rec 18–2.

2 See Ch 19.

3 See Ch 28. Data breach notification is discussed in Ch 51.

'Accountability' principle

Background

32.3 Accountability principles provide a framework through which requirements for the handling of personal information can be enforced. Most commonly, accountability principles require a regulated entity to identify a person or persons who will take responsibility for that entity's compliance. For example, the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines) provide that 'a data controller should be accountable for complying with measures which give effect to the [other] principles [in the OECD Guidelines]'.[4]

32.4 Accountability principles also may require a regulated entity, in certain circumstances, to retain responsibility for personal information that it transfers to third parties. For example, Canadian privacy law provides:

> An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.[5]

32.5 The IPPs and the NPPs do not include a specific privacy principle dealing with accountability. Some other provisions of the *Privacy Act 1988* (Cth), however, are relevant to an accountability framework. In particular, ss 13 and 13A establish that, where an agency or organisation is in breach of the privacy principles, this constitutes an interference with privacy. Such a breach triggers the availability of a number of avenues to enforce compliance.[6]

32.6 Under IPP 4, agencies are required to take steps to protect personal information that they transfer to third parties. This principle provides, in part, that:

> if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper [must be] done to prevent unauthorised use or disclosure of information contained in the record.[7]

---

4 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 14. See, also: *Federal Data Protection Act 1990* (Germany) ss 4f, 4g; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principle 4.1.

5 See *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principle 4.1.

6 Compliance with, and enforcement of, the requirements in the privacy principles are discussed in Part F.

7 *Privacy Act 1988* (Cth) s 14, IPP 4.

32.7 Section 95B of the *Privacy Act* also requires an agency that enters into a Commonwealth contract to take contractual measures to ensure that a service provider acts in accordance with the IPPs.[8]

32.8 The NPPs do not include an equivalent 'contractors' requirement. NPP 9, however, prohibits an organisation from transferring personal information overseas unless a number of conditions are satisfied. These include where the organisation:

- reasonably believes that the recipient of the information is subject to principles for fair handling of the information that are substantially similar to the NPPs; or

- has taken steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient inconsistently with the NPPs. [9]

Submissions and consultations

32.9 Some stakeholders supported the inclusion of a specific privacy principle in the model UPPs dealing with accountability.[10] Smartnet, for example, noted that individuals do not want their personal information to be passed on or used for an unintended purpose. It suggested that the most appropriate solution to this

> is to require the initial collecting organisation to remain accountable for the use and protection of all information it collects, even when that information has been transferred to another party.[11]

32.10 The Australian Federal Police and the National Health and Medical Research Council, however, specifically opposed the addition of an 'Accountability' principle.[12] The Office of the Privacy Commissioner (OPC) submitted that

> agencies and organisations [should] incorporate privacy into their decision-making, policies and culture through non-legislative solutions. For example … agencies [may] nominate … a 'privacy contact officer' to provide expert guidance on privacy issues and serve as the first point of contact for privacy questions within the agency. In the private sector, the privacy connections network provides a forum for developing and promoting good privacy practice.[13]

---

8 Commonwealth contracts are discussed in Ch 14.

9 *Privacy Act 1988* (Cth) sch 3, NPP 9. This principle is discussed in Ch 31.

10 National Association for Information Destruction, *Submission PR 133*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007.

11 Smartnet, *Submission PR 457*, 11 December 2007.

12 Australian Federal Police, *Submission PR 186*, 9 February 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

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

32.11 The Cyberspace Law and Policy Centre questioned the practical utility of an 'Accountability' principle and commented that the existing models of this principle 'seem to add little substance' to current privacy protections.[14]

ALRC's view

32.12 The ALRC does not support the inclusion of a discrete 'Accountability' principle in the model UPPs. Ensuring that agencies and organisations are accountable for their handling of personal information can be better achieved in other ways.

32.13 In this Report, the ALRC makes a number of recommendations to improve compliance with the *Privacy Act* by agencies and organisations—in particular, by enhancing the powers of the Privacy Commissioner to investigate and resolve privacy complaints.[15] In addition, the ALRC recommends establishing a statutory cause of action for serious invasions of privacy.[16] Accountability for personal information handling also will be promoted through the ALRC's recommended data breach notification provisions.[17]

32.14 Issues of accountability often arise where an agency or organisation subcontracts the handling of personal information to an entity that is not bound by the *Privacy Act*. In this Report, the ALRC recommends removing a number of the current exemptions from the *Privacy Act*—most relevantly, the small business exemption.[18]

32.15 Accountability also is central to the ALRC's recommended 'Cross-border Data Flows' principle. In particular, this principle establishes accountability as the default position in relation to cross-border data flows. An agency or organisation will be responsible under the *Privacy Act* for the acts and practices of a recipient of personal information that is the subject of a cross-border transfer unless one of the three exceptions applies.[19]

32.16 Provided these recommendations are implemented, there will be few, if any, situations where an agency or organisation is not responsible for handling personal information in accordance with the *Privacy Act*.

'Prevention of Harm' principle

Background

32.17 There is a question about whether the model UPPs should contain a 'Prevention of Harm' principle. Such a provision would require agencies and organisations 'to

---

14 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
15 See Chs 49, 50.
16 See Ch 74.
17 See Ch 51.
18 See Ch 39.
19 See Ch 31.

prevent tangible harms to individuals and to provide for appropriate recovery for those harms if they occur'.[20]

32.18 The Asia-Pacific Economic Cooperation Privacy Framework,[21] for example, states:

> Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.[22]

Submissions and consultations

32.19 Some stakeholders supported the inclusion of a specific privacy principle in the model UPPs dealing with the prevention of harm.[23] Veda Advantage submitted that this aligns with the overall 'purpose of regulating information flows, [which] is to protect individuals from harmful uses of information'.[24]

32.20 The majority of stakeholders that commented on this issue, however, opposed a 'Prevention of Harm' principle.[25] One stakeholder argued that this is an unsuitable subject to be addressed in a privacy principle.

> The sentiment that privacy remedies should concentrate on preventing harm … is unexceptional but it is strange to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other Principles makes it easier to justify exempting whole sectors (eg small business in Australia's law) as not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the USA).[26]

---

20 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341, 368.

21 This Framework is discussed in Ch 31.

22 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 1.

23 Government of South Australia, *Submission PR 187*, 12 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

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

25 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; AAMI, *Submission PR 147*, 29 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

26 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007, citing G Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 91, 100.

32.21 The Law Council of Australia was concerned that such a principle would be too imprecise because it is difficult to articulate a precise meaning of 'harm'.

> While financial harm and damage to reputation or character are concepts which are well understood, other concepts of harm which are raised within the privacy debate such as 'distress' and the knowledge that someone has their personal information are harder to place within a legislative context.[27]

ALRC's view

32.22 A number of the principles in the model UPPs already incorporate a harm prevention approach. In particular, the 'Data Quality' principle and the 'Data Security' principle impose specific obligations to ensure the integrity of personal information that is handled by agencies and organisations, and to guard against possible misuse and unauthorised disclosure.[28] The 'Anonymity and Pseudonymity' principle also aims to lessen the threat of personal information being misused by reducing the amount of personal information that agencies and organisations collect.[29] Finally, the obligations imposed by a general 'Prevention of Harm' principle could be undesirably vague. Accordingly, the ALRC does not support including such a principle in the model UPPs.

'No Disadvantage' principle

Background

32.23 During the course of the Inquiry, stakeholders suggested that a 'No Disadvantage' principle or provision should be included in the *Privacy Act*. That is, a provision prohibiting agencies and organisations from unfairly disadvantaging an individual on the basis that he or she is seeking to assert his or her privacy rights. In the context of the 'Anonymity and Pseudonymity' principle, for example, unfavourable treatment may include the organisation charging a fee that only would apply to individuals who seek to conduct transactions anonymously, or withholding a product or service until the individual decides that he or she no longer wishes to conduct transactions anonymously.

32.24 The *Privacy Act* currently does not contain an express 'no disadvantage' provision. There is no such provision in the privacy legislation of any other Australian jurisdiction; nor is there such a provision in the OECD Guidelines or in the privacy legislation of other common law jurisdictions, such as the United Kingdom, Canada and the United States. The draft Asia-Pacific Privacy Charter, however, contains a 'Non-discrimination' principle that states:

> People should not be denied goods or services or offered them on unreasonably disadvantageous terms (including higher cost) in order to enjoy the rights described in this Charter.

---

27 Law Council of Australia, *Submission PR 177*, 8 February 2007.
28 Data quality and data security are discussed in Chs 27 and 28 respectively.
29 See Ch 20.

> The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.[30]

32.25 While the *Privacy Act* currently does not contain a specific 'No Disadvantage' provision, some of its provisions are directed towards a similar policy goal. For example, NPP 6.4 states:

> If an organisation charges for providing access to personal information, those charges:
>
> (a) must not be excessive; and
>
> (b) must not apply to lodging a request for access.[31]

32.26 A number of the IPPs and NPPs require agencies and organisations, respectively, to take 'reasonable steps' to protect individuals' privacy rights.[32] Where asserting such privacy rights results in unfavourable treatment—for example, through the imposition of a fee—this may indicate that it is not a 'reasonable step' on the part of the agency or organisation.

Submissions and consultations

32.27 Privacy advocates supported the addition of a 'No Disadvantage' principle.[33] The Australian Privacy Foundation, for example, submitted that this would 'ensure that data users do not use pricing or other sanctions to deter individuals from exercising their privacy rights'.[34] The Cyberspace Law and Policy Centre stated:

> without a broader 'no disadvantage' principle, it is all too easy for data users to levy a charge for the exercise of privacy choices and rights, either directly, or by differential pricing, or to impose some other non-financial barrier.[35]

32.28 The Centre accepted that, if such a principle was not included as a separate principle in the model UPPs, the concept usefully could be incorporated into other privacy principles; in particular, through the requirement that agencies and organisations take 'reasonable steps' to protect individuals' information privacy.[36] The

---

30 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 5 May 2008, Principle 5. A similar provision is included in the Australian Privacy Charter: Australian Privacy Foundation, *Australian Privacy Charter* <www.privacy.org.au/About/PrivacyCharter.html> at 31 July 2007, Principle 18.

31 Agencies are not permitted to charge individuals for access to personal information that an agency holds about them. See Ch 29.

32 See *Privacy Act 1988* (Cth): s 14, IPPs 2, 3, 4, 5.1, 7, 8; and sch 3, NPPs 1.3, 1.5, 3, 4, 5.2.

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

34 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

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

36 Ibid.

OPC also supported incorporating the concept of 'no disadvantage' into other privacy principles.[37]

ALRC's view

32.29 Individuals should not be disadvantaged unfairly by seeking to assert their privacy rights. In the ALRC's view, however, a separate 'No Disadvantage' principle in the model UPPs is not the most appropriate vehicle to achieve this policy outcome. Instead, this concept should be incorporated, where appropriate, into other privacy principles.

32.30 Some privacy principles already include a 'no disadvantage' element. In particular, NPP 6.4 prohibits an organisation from charging excessive fees in respect of access to, and correction of, personal information held by the organisation. The ALRC recommends that this provision be retained in the model 'Access and Correction' principle.[38] Moreover, agencies currently are not permitted under the *Privacy Act* to charge individuals for access to personal information that the agency holds about them. The ALRC recommends that this position continue.[39]

32.31 The ALRC also recommends that, if an individual requests access to an agency's or organisation's Privacy Policy, the agency or organisation must take reasonable steps to make this available without charge.[40]

32.32 More generally, the 'no disadvantage' concept can be incorporated into the privacy principles through the obligation on agencies and organisations to take 'reasonable steps' to protect individuals' information privacy. For example, the 'Data Security' principle requires agencies and organisations to take reasonable steps to destroy or render non-identifiable personal information that they no longer need.[41] This requirement should be interpreted to mean that costs associated with destroying or rendering the information non-identifiable should be treated as normal operating costs of the agency or organisation in question, and not a cost imposed on the individual involved.

32.33 Similarly, the 'Anonymity and Pseudonymity' principle states that, wherever it is lawful and practicable, agencies and organisations must give individuals the clear option of transacting anonymously or pseudonymously.[42] Implicit in this requirement is that agencies and organisations must not impose unreasonable disincentives on individuals seeking to exercise this option. For example, it would not be reasonable for

---

37 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
38 See Ch 29.
39 Charging for access to personal information held by agencies is discussed in Ch 29.
40 See Ch 24.
41 See Ch 28. Note also that a similar obligation already applies to organisations: *Privacy Act 1988* (Cth) sch 3, NPP 4.2.
42 See Ch 20.

individuals to be charged a punitive fee for choosing to remain anonymous in their transactions with an agency or organisation.

32.34 Finally, the ALRC's recommendation, that the *Telecommunications Act 1997* (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number, is also underpinned by the concept of 'no disadvantage'.[43]

43 Rec 72–17.

Part E

Exemptions

33. Overview: Exemptions from the *Privacy Act*

Contents

Introduction

33.1 The application of the *Privacy Act 1988* (Cth) is limited by a number of exemptions and exceptions. This Report distinguishes between exemptions and partial exemptions to the requirements set out in the *Privacy Act*, and exceptions to the privacy principles.[1] An *exemption* applies where a specified entity or a class of entity is not required to comply with any of the requirements in the *Privacy Act*. For example, intelligence agencies, such as the Australian Security Intelligence Organisation (ASIO), are exempt from compliance with the provisions of the *Privacy Act*. A *partial exemption* applies where a specified entity or a class of entity is required to comply with either: some, but not all, of the provisions of the *Privacy Act*; or some or all of the provisions of the *Privacy Act*, but only in relation to certain of its activities. For

1 Compare B Stewart, 'The New Privacy Laws: Exemptions and Exceptions to Privacy' (Paper presented at The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

example, the federal courts are *partially exempt* as they only are required to comply with the *Privacy Act* in relation to their administrative activities. An *exception* to the privacy principles operates where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. For example, there is an exception to the prohibition against an organisation using or disclosing personal information for a secondary purpose where the individual in question has given his or her consent.[2]

33.2 This chapter provides an overview of the exemption provisions in the *Privacy Act*, outlines the exemptions under international instruments and considers issues concerning the existing exemptions from the Act. The remaining chapters in Part E examine specific exemptions from the *Privacy Act* in the public and private sectors, and consider whether new exemptions or exceptions should be included in the Act. The broad application of exceptions to the privacy principles is discussed in Part D.

Privacy Act exemptions

33.3 There are a number of ways in which entities can be exempt, either completely or partially, from the *Privacy Act*. Under the existing law, entities may be exempt from the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs) (or an approved privacy code),[3] the tax file number provisions or the credit reporting provisions of the Act.

33.4 Broadly speaking, the IPPs apply to acts and practices of Australian Government agencies and the NPPs apply to acts and practices of private sector organisations.[4] Entities that fall within the definition of an 'agency' therefore will be bound by the IPPs; and those that fall within the definition of an 'organisation' will be bound by the NPPs. The structural reform of the IPPs and NPPs is discussed in Chapter 18.

33.5 Where entities fall within the definition of an 'agency' or an 'organisation', their acts and practices may still be exempt from the *Privacy Act* if those acts or practices are excluded expressly from the reference to an 'act or practice' to which the Act applies. Under s 7 of the Act, a reference to an 'act or practice' is generally a reference to an act done, or a practice engaged in, by: an agency; a tax file number recipient; a credit reporting agency; or a credit provider. The section, however, excludes a wide range of activities of certain specified entities. For example, while federal courts fall within the definition of an 'agency' under the Act, their acts and practices only are covered by the IPPs if they relate to administrative matters.[5] Any activity of the courts

---

2 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(b).

3 Where the Privacy Commissioner has approved a privacy code for a particular organisation or industry, it replaces the NPPs for those organisations that are bound by the code. To the extent that an organisation is not bound by such a code, it is bound by the NPPs: Ibid s 16A(2).

4 Ibid ss 16, 16A.

5 Ibid ss 6(1), 7(1)(a)(ii), (b).

that relates to non-administrative matters falls outside the reference to 'act or practice' in the *Privacy Act* and, therefore, is exempt from the Act.

33.6 Part IIIA of the *Privacy Act* regulates the handling of credit information about individuals by credit reporting agencies and credit providers. Individuals and entities are exempt from the credit reporting provisions where they fall outside the definition of a 'credit reporting agency' or a 'credit provider', or where their acts and practices are excluded by s 7 of the Act. Credit reporting is discussed in Part G.

Public sector exemptions

33.7 The *Privacy Act* prohibits an agency from engaging in an act or practice that breaches the IPPs.[6] Agencies include: Australian Government ministers and departments; bodies and tribunals established or appointed for a public purpose by or under Commonwealth and ACT laws; Australian Government statutory office holders and administrative appointees; federal courts; and the Australian Federal Police (AFP). The definition of agency excludes incorporated companies, societies and associations, even if they are established under Commonwealth law.[7]

33.8 Agencies are not subject to the *private sector* provisions of the Act unless they have been prescribed by regulation.[8] An agency also may be subject to the tax file number provisions and the credit reporting provisions of the Act in some circumstances.[9]

33.9 The definition of agency excludes an organisation within the meaning of the *Conciliation and Arbitration Act 1904* (Cth) (now repealed)[10] and a branch of such an organisation.[11] This refers to federally registrable employer and employee associations and federally registrable enterprise associations.[12] In Chapter 5, the ALRC recommends that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity.[13] Since the *Conciliation and Arbitration Act* has been repealed, this provision should be updated as part of the recommended amendment of the Act.

33.10 Any act or practice engaged in by, or information disclosed to, a person in the course of employment by, or in the service of, an agency is treated as having been done by, engaged in by, or disclosed to, the agency.[14] A person is not to be regarded as an

---

6 Ibid s 16.
7 Ibid s 6(1).
8 Ibid ss 6C, 7A, 16A.
9 Ibid ss 11, 11A, 11B.
10 The *Conciliation and Arbitration Act 1904* (Cth) was repealed by s 3 of the *Industrial Relations (Consequential Provisions) Act 1988* (Cth).
11 *Privacy Act 1988* (Cth) s 6(1).
12 *Workplace Relations Act 1996* (Cth) sch 2, cl 18.
13 Rec 5–2.
14 *Privacy Act 1988* (Cth) s 8.

agency, however, merely because he or she is the holder of, or performs the duties of: a judge or magistrate; a member of a prescribed Commonwealth tribunal; a prescribed office under the *Privacy Act* or the *Freedom of Information Act 1982* (Cth) (FOI Act);[15] or an office established under a Commonwealth or ACT law for the purposes of an agency.[16]

33.11 Chapters 34–38 discuss agencies that are completely or partially exempt from the *Privacy Act*—namely, defence and intelligence agencies, federal courts and tribunals, specified agencies that are exempt under the FOI Act, certain agencies with law enforcement functions, and others.

Private sector exemptions

33.12 Under existing law, the NPPs bind entities that fall within the definition of an 'organisation'.[17] An 'organisation' is defined as an individual, a body corporate,[18] a partnership,[19] any other unincorporated association,[20] or a trust[21] that is not otherwise exempt from the operation of the *Privacy Act*.[22] Certain entities are specifically excluded from the definition of 'organisation' and are, therefore, exempt from the Act. These exempt entities include small business operators, registered political parties, agencies, state and territory authorities, and prescribed state and territory instrumentalities.[23]

33.13 Certain acts and practices of organisations also fall outside the operation of the *Privacy Act*. There are five ways in which an act or practice may be excluded from the Act. An act or practice may be excluded from:

- what constitutes a breach of the NPPs or an approved privacy code;

---

15 No such offices have been prescribed under either Act.

16 *Privacy Act 1988* (Cth) s 6(5).

17 Ibid s 16A.

18 A body corporate is 'any entity that has a legal personality under Australian law or the law of another country': Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 6.

19 An act done, or a practice engaged in, by one of the partners in a partnership is deemed to be an act or practice of the organisation. The *Privacy Act 1988* (Cth) imposes obligations on each partner but they may be discharged by any of the partners: Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 6.

20 An unincorporated association includes a cooperative. The *Privacy Act 1988* (Cth) also covers acts or practices engaged in by an individual in his or her capacity as a member of the cooperative's committee of management. The *Privacy Act* imposes obligations on each member of the committee of management but they may be discharged by any of the members of that committee: Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 6.

21 An act or practice engaged in by a trustee is taken to have been engaged in by the trust. Obligations under the *Privacy Act 1988* (Cth) are imposed on each trustee but may be discharged by any of the trustees: Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 6.

22 *Privacy Act 1988* (Cth) s 6C(1).

23 Ibid s 6C(1).

- what constitutes an interference with the privacy of an individual;
- the [reference to] an 'act or practice';
- the operation of the Act; or
- the operations of the NPPs.[24]

33.14 Chapters 39–43 examine current exemptions from the *Privacy Act* that apply to organisations, including the small business exemption, the employee records exemption, the journalism exemption, the political exemption and other private sector exemptions. Chapter 44 considers whether new exemptions or exceptions should be introduced.

Exemptions under international instruments

OECD Guidelines

33.15 The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines) do not refer to exemptions.[25] They do provide expressly, however, for the possibility of excluding personal data from the application of the Guidelines that 'obviously do not contain any risk to privacy and individual liberties'.[26]

33.16 In addition, the OECD Guidelines recognise that there may be exceptions to the privacy principles. OECD Guideline 4 provides two general criteria to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible; and they should be made known to the public.[27] Acceptable bases for exceptions set out in the OECD Guidelines include national sovereignty, national security, public policy and the financial interests of the state.[28] Importantly, the OECD Guidelines state that exceptions should be limited to those that are necessary in a democratic society.[29]

33.17 The Memorandum to the OECD Guidelines acknowledges that opinions may vary on the question of exceptions. It recognises that member countries may apply the

---

24 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [1-650].

25 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

26 Ibid, Guideline 3(b).

27 Ibid, Guideline 4.

28 Ibid; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), Guideline 4; Memorandum, [46].

29 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Memorandum, [47].

Guidelines differently to particular kinds of personal data or in particular contexts, for example, credit reporting, criminal investigation and banking.[30]

33.18 The OECD Guidelines also recognise that the application of the Guidelines is subject to various constitutional limitations in countries with a federal system and therefore there are no requirements to apply the Guidelines beyond the limits of constitutional competence.[31] The Australian Parliament's power under the *Australian Constitution* to enact federal privacy laws is discussed in Chapter 3.

EU Directive

33.19 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament contains a number of specific exemptions and exceptions.[32] Exemptions in the EU Directive include the processing of data by: natural persons in the course of a purely personal or household activity;[33] and political parties in compiling data on individuals' political opinions in the course of electoral activities.[34]

33.20 Examples of exceptions to the privacy principles in the EU Directive include processing of data: necessary for the prevention, investigation, detection and prosecution of criminal offences;[35] concerning public security, defence, state security (including the economic well-being of the state when the processing operation relates to state security matters) and the activities of the state in areas of criminal law;[36] and for journalistic purposes or the purpose of artistic or literary expression if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[37]

APEC Privacy Framework

33.21 Under the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, exceptions to privacy principles are to be: 'limited and proportional to meeting the objectives to which the exceptions relate'; made known to the public; or in accordance with law.[38]

33.22 The APEC Privacy Framework defines 'personal information controller' to exclude an individual who deals with personal information in connection with his or

---

30 Ibid, Memorandum, [19(g)], [47].
31 Ibid, Guideline 5; Memorandum, [48].
32 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).
33 Ibid, art 3(2).
34 Ibid, recital 36.
35 Ibid, art 13(1)(d).
36 Ibid, art 3(2).
37 Ibid, art 9. See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recitals 17, 37.
38 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

her personal, family or household affairs.[39] Like the EU Directive, the APEC Privacy Framework is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy interests.[40] Unlike the EU Directive, the APEC Privacy Framework does not contain exceptions for journalistic, literary or artistic expression, or an exemption for political parties in respect of their political or electoral activities.

Should there be any exemptions from the *Privacy Act*?

33.23 Before examining whether the existing exemptions from the operation of the *Privacy Act* are appropriate, the threshold question is whether the Act should contain any exemptions at all. Professor Roger Clarke has suggested that there should be no exemptions from the privacy principles. In his view, privacy principles should be universal statements that convey the idea that the principles are paramount. The manner in which they are formulated and applied in practice should involve careful balancing between privacy and other interests so that the principles are not infringed. He argues that powerful interests are protected through large numbers of 'vague and extensible' exemptions, and that privacy protection is lost entirely once a class of organisation or activity is exempted from the privacy principles.[41]

33.24 Blair Stewart, of the Office of the Privacy Commissioner, New Zealand, has taken a different view.[42] He concedes that well-drafted exceptions to specific privacy principles are preferable to excluding an entire class of entities or information. Stewart argues, however, that some types of entities and information should be excluded from the coverage of privacy principles so that the principles remain 'workable, general and not overly complex'—for example, it might be better not to apply some principles to intelligence agencies than to have exceptions for national security provided throughout the principles.[43]

33.25 Privacy legislation in some overseas jurisdictions contains full or partial exemptions relating to, for example, personal information handled by: individuals for

39 Ibid, [10].
40 Ibid, [13].
41 R Clarke, *Exemptions from General Principles Versus Balanced Implementation of Universal Principles* (1998) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Except.html> at 31 March 2008.
42 B Stewart, 'The New Privacy Laws: Exemptions and Exceptions to Privacy' (Paper presented at The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).
43 Ibid, 10.

the purposes of their personal, family or household affairs;[44] intelligence agencies;[45] and news media in relation to journalism or news activities.[46]

33.26 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC noted stakeholder views that there should be few, if any, blanket exemptions from the *Privacy Act*.[47] For example, the Office of the Victoria Privacy Commissioner (OVPC) submitted that entities should not be completely exempt. It suggested that exemptions or exceptions should be targeted at particular practices, and that some principles should apply universally. The OVPC stated that privacy legislation 'should only be subject to such reasonable limits … as can be demonstrably justified in a free and democratic society'.[48] Other stakeholders suggested that only a limited number of entities should be exempt. Exemptions that have been suggested as justifiable include individuals handling personal information solely for non-business purposes, entities that are subject to equivalent privacy laws (such as state and territory authorities),[49] and defence and intelligence agencies.[50]

33.27 In contrast, a few stakeholders specifically stated that it is appropriate to have exemptions from the *Privacy Act*.[51] For instance, while both the Australian Broadcasting Corporation (ABC) and the Special Broadcasting Service (SBS) submitted that there should be few blanket exemptions from the *Privacy Act*, they suggested that the EU Directive and other international instruments illustrate a number of clear policy reasons why certain exemptions should be maintained. The ABC submitted that many, if not all, of the exemptions under the Act are based on similar policy concerns to those reflected in international instruments.[52] SBS stated that the justification for exemptions that are common to all international instruments is the need

---

44 See, eg, *Data Protection Act 1998* (UK) s 36; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(2)(b); *Personal Data Act 1998* (Sweden) s 6; *Privacy Act 1993* (NZ) s 56; *Personal Data (Privacy) Ordinance* (Hong Kong) s 52.

45 See, eg, *Privacy Act 1974* 5 USC § 552a (US) (j)(1); *Privacy Act 1993* (NZ) s 57. See also *Personal Data (Privacy) Ordinance* (Hong Kong) s 57 (exemption of personal data held by or on behalf of the government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong).

46 See, eg, *Privacy Act 1993* (NZ) s 2(1) (definition of 'agency'); *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

47 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 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; SBS, *Submission PR 112*, 15 January 2007; K Pospisek, *Submission PR 104*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.

48 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

49 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.

50 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Confidential, *Submission PR 143*, 24 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007.

51 SBS, *Submission PR 112*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

52 Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.

to balance privacy rights against a public interest purpose, such as matters essential to law and governance and freedom of expression.[53]

33.28 The ABC and SBS also submitted that, in the interest of certainty, exemptions are preferable to exceptions to specific privacy principles.[54] The ABC stated that targeted exemptions could reflect a careful balancing of privacy and other interests.[55] SBS suggested that a universal statement of principles would be unworkable, as it would result in uncertainty and extensive litigation before the application of the principles could be understood.[56]

33.29 The Real Estate Institute of Australia (REIA) took the view that subjecting entities to overly rigorous privacy protection, regardless of the risk to individual privacy or the context in which the entity operates, may impinge on the ability of certain entities to carry out activities that are in the national interest. It submitted that such an approach also would result in an unnecessary and disproportionate compliance burden that would be passed on to consumers by way of increased prices.[57] The Fundraising Institute—Australia Ltd expressed a contrary view, submitting that the exemption for commercial entities, such as small business operators, undermines public confidence that the *Privacy Act* will protect personal information adequately.[58]

33.30 In DP 72, the ALRC expressed the preliminary view that exemptions from the *Privacy Act* may be necessary for those entities the principal function of which is in direct conflict with privacy principles, and for those entities that require specific information-handling standards in order to balance privacy interests with other public interests. The ALRC considered that exemptions for these entities would be appropriate, provided that there are other information-handling standards that apply to the exempted entity. In addition, the ALRC expressed the view that entities that are subject to obligations that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act*, should be exempt from the Act—as the need to comply with two equivalent regimes would add unnecessarily to the compliance burden for such entities.

---

53 SBS, *Submission PR 112*, 15 January 2007.
54 Ibid; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.
55 Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.
56 SBS, *Submission PR 112*, 15 January 2007.
57 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.
58 Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007.

Submissions and consultations

33.31 Submissions indicated support for limiting exemptions from the *Privacy Act*.[59] Liberty Victoria submitted that privacy principles should be applied uniformly and there should be no exemptions from the *Privacy Act*.[60]

33.32 The Law Society of New South Wales submitted that exemptions should be limited. It stated that 'traditional areas benefiting from exemptions and exceptions should be re-examined and assessed against expressed criteria as detailed in the Act or regulations', and those criteria should, in turn, be reviewed for their suitability. The Law Society also suggested that where an exemption or exception is justified, the exempted activity should be covered by other legislation that specifies a date for review and is subject to a privacy impact assessment, so that there would be some debate in both the community and the Parliament before an exemption or exception is granted.[61]

33.33 Privacy NSW considered that exemptions are 'blunt instruments', and that the balancing of privacy interests with other public interests 'can best be achieved by the use of exemptions limited to the functions of the agency or organisations'. It supported the use of partial exemptions that are targeted at particular practices and provide some privacy protection for the personal information of employees, on the basis that:

> the use of blanket exemptions presents a risk that employees of some agencies may have lesser rights than others and that the exemption will excise whole categories of dealings which do not relate to the purpose of exemption.[62]

ALRC's view

33.34 Privacy interests in some cases may be outweighed by other public interests, such as national security, the administration of justice and the free flow of information to the public by the media. The purpose of having exemption provisions is to balance the need to protect privacy against these other interests, as is reflected in international instruments.

33.35 A blanket exemption from privacy legislation is a blunt instrument, in that it exempts all activities of a specified entity or class of entities, regardless of whether the particular activity relates to the conflicting public interest. There are some entities, however, such as intelligence agencies and specialist law enforcement agencies, the principal function of which is in direct conflict with a number of the privacy principles. In addition, due to the sensitive nature of the operation of these entities, oversight

---

59 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

60 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.

61 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

62 Privacy NSW, *Submission PR 468*, 14 December 2007.

bodies—such as the Inspector-General of Intelligence and Security (IGIS) and parliamentary joint committees—have been established specifically to oversee their operations.[63] Other entities, such as royal commissions, inquire into matters of public interest and, therefore, should have their own information-handling standards tailored to their special role.[64] In these cases, the exemption of these entities from the operation of the *Privacy Act* is appropriate, provided that there are other information-handling standards, such as ministerial privacy guidelines, that apply to the exempted entity. These standards should reflect the model Unified Privacy Principles (UPPs) to the extent that this is possible.

33.36 In other instances, a partial exemption from the operation of the *Privacy Act* may be appropriate, where it would be possible to distinguish between the activities of an agency or organisation that conflict with privacy interests and those that do not. For example, federal courts require special information-handling rules that balance privacy interests with the principle of open justice. There is, however, no sound policy reason why their acts and practices in respect of non-administrative matters, such as their handling of the employment records of court staff, should be exempt from the *Privacy Act*.[65] In the case of media organisations, the public interest in the free flow of information to the public only relates to the journalistic activities of media organisations. Therefore, the exemption that applies to acts and practices in the course of journalism should not apply more broadly to information that does not constitute news, current affairs or documentaries, unless the public interest in the dissemination of that information outweighs privacy interests.[66]

The number and scope of exemptions

The number of exemptions

33.37 The *Privacy Act* has been criticised for the large number of exemptions it contains.[67] In the public sector, there are three classes of agencies—federal courts, ministers and royal commissions—and more than 20 specific, named agencies that are partially or completely exempt from the operation of the Act. In the private sector, in addition to the four exempt classes of entities—namely, small business operators, registered political parties, state and territory authorities, and prescribed state and

63 See Chs 34, 37.
64 See Ch 38.
65 See Ch 35.
66 See Rec 42–1.
67 R Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (1989) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html> at 14 April 2008; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 3 September 2000.

territory instrumentalities—there are eight categories of organisations that are exempt from the Act.[68]

33.38 The OECD Guidelines state that exceptions to the privacy principles should be 'as few as possible'.[69] Similarly, under the APEC Privacy Framework, exceptions to the principles are to be 'limited and proportional to meeting the objectives to which the exceptions relate'.[70]

33.39 One commentator has expressed the view that keeping exemptions to a minimum, and limiting them to particular provisions of the law whenever possible, is important to ensure that privacy protection applies as widely as possible throughout the community.[71] Another commentator argued that the effect of the large number of private sector exemptions in the *Privacy Act* is to validate the data processing practices of certain organisations, thus failing to protect the privacy of individuals adequately.[72]

33.40 Privacy legislation in some jurisdictions contains significantly fewer exemptions than the *Privacy Act*. For example, there are four exemptions in the privacy legislation in force in the United Kingdom,[73] 15 in New Zealand,[74] and three in Hong Kong.[75]

---

68 *Privacy Act 1988* (Cth) s 7B(1) (individuals acting in a non-business capacity), s 7B(2) (contracted service providers for a Commonwealth contract), s 7B(3) (current or former employers of an individual), s 7B(4) (media organisations), s 7B(5) (contracted service providers for a state contract); s 7C (political representatives); s 13B (related bodies corporate); s 13C (partnerships).

69 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 4(a).

70 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

71 N Waters, 'Essential Elements of a New Privacy Act' (1999) 5 *Privacy Law & Policy Reporter* 168, 168.

72 H Lloyd, 'Are Privacy Laws More Concerned with Legitimising the Data Processing Practices of Organisations than with Safeguarding the Privacy of Individuals?' (2002) 9 *Privacy Law & Policy Reporter* 81.

73 *Data Protection Act 1998* (UK) s 30(2) (personal data in respect of which the data controller is a proprietor of, or a teacher at, a school; or an education authority in Scotland), s 30(3) (personal data processed by government departments, local authorities, voluntary organisations or other bodies in the context of carrying out social work), s 31 (personal data processed for the purposes of discharging functions relating to regulatory activity), s 36 (personal data processed by individuals for the purposes of their family or household affairs, including recreational purposes). Note that, although Schedule 7 to the Act is entitled 'Miscellaneous Exemptions', the provisions in that schedule are exceptions to specific data protection principles, rather than exemptions.

74 *Privacy Act 1993* (NZ) s 2(1) (the term 'agency' does not include: the Sovereign; the Governor-General or the Administrator of the Government; the House of Representatives; a member of Parliament in his or her official capacity; the Parliamentary Service Commission; the Parliamentary Service (with certain exceptions); in relation to its judicial functions, a court; in relation to its judicial functions, a tribunal; an Ombudsman; a Royal Commission; a commission of inquiry appointed under the *Commissions of Inquiry Act 1908* (NZ); a commission, board, court or committee of inquiry appointed by statute to inquire into a specified matter; or in relation to its news activities, any news medium), s 56 (personal information held by individuals for the purposes of their personal, family, or household affairs), s 57 (information held by intelligence organisations).

75 *Personal Data (Privacy) Ordinance* (Hong Kong) s 52 (personal data held by individuals for the management of their personal, family or household affairs or for recreational purposes), s 57 (personal data held by or on behalf of the government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong), s 61 (personal data held by a data user whose business consists of a news activity and solely for the purpose of that activity). Note that, although Part VIII of the Ordinance is entitled 'Exemptions', some of the provisions in that part are exceptions to the data

Although there are some exemptions common to both Australia and comparable jurisdictions—such as exemptions relating to personal use, national security, defence and journalism—a number of exemptions from the *Privacy Act* are not provided for in other jurisdictions. For example, contrary to the position in Australia, legislation in the United Kingdom, Canada and Hong Kong does not contain exemptions for specified government bodies, such as defence agencies and Auditors-General.[76] In the United Kingdom, Canada and New Zealand, there is no exemption that applies to small businesses, employee records, registered political parties, or political acts and practices.[77]

33.41 In DP 72, the ALRC noted that stakeholders often expressed the concern that there are too many exemptions from the *Privacy Act*.[78] The Office of the Privacy Commissioner (OPC) submitted that exemptions under the *Privacy Act* should be minimised in order to achieve uniformity and consistency of application of privacy legislation, and that a clear public interest for the exemptions should exist to support their creation or continuation. The OPC suggested that 'existing exemptions contained in the *Privacy Act* have developed over time and in some instances may require review to assess their continuing suitability'.[79]

33.42 The Centre for Law and Genetics also submitted that the substantial number of exemptions have the potential to undermine the operation of the privacy principles and compromise the privacy of individuals.[80] Similarly, the Legal Aid Commission of New South Wales submitted that 'the Act would be more effective if there were fewer exemptions, but a more flexible approach to applying the principles to different circumstances'.[81]

The scope of the exemptions

33.43 In relation to the public sector, the acts and practices of some agencies—namely, the Australian Crime Commission (ACC), the Integrity Commissioner or a staff member of the Australian Commission for Law Enforcement Integrity, royal commissions, the Commission of inquiry into the 2007 equine influenza outbreak and

protection principles, rather than exemptions: see, eg, *Personal Data (Privacy) Ordinance* (Hong Kong) s 53 (employment—staff planning), s 60 (legal professional privilege), s 62 (statistics and research).

76 *Data Protection Act 1998* (UK); *Privacy Act* RS 1985, c P-21 (Canada); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada); *Personal Data (Privacy) Ordinance* (Hong Kong).

77 *Data Protection Act 1998* (UK); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada); *Privacy Act 1993* (NZ).

78 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

79 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

80 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

81 Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

certain intelligence agencies—are completely exempt from the *Privacy Act*.[82] The relevant intelligence agencies are defined as the Australian Secret Intelligence Service (ASIS), ASIO and the Office of National Assessments (ONA).[83]

33.44 In relation to the private sector, certain entities are excluded specifically from the definition of 'organisation' and therefore are exempt from compliance with the NPPs, unless they fall within one of the conditions under which the exemption does not apply. These entities include small business operators, registered political parties, state and territory authorities, and prescribed state and territory instrumentalities.[84] As a result, a large number of entities are exempt from the *Privacy Act*. The Australian Government Department of Employment, Workplace Relations and Small Business has estimated that approximately 94% of businesses may be exempt from the private sector provisions of the Act.[85]

33.45 Professor Graham Greenleaf and Nigel Waters have suggested that blanket exemptions for whole classes of agencies and organisations are undesirable.[86] Clarke has argued that any form of exemption creates a risk insofar as 'it creates a void within which uncontrolled abuses can occur'.[87]

33.46 It also has been suggested that some of the exemption provisions are expressed too broadly.[88] For example, acts and practices of a media organisation done 'in the course of journalism' are exempt from the *Privacy Act*.[89] Under the Act, a 'media organisation' is an organisation that collects, prepares or disseminates materials having the character of news, current affairs, information or documentaries to the public; or

---

82 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (iiia), (iv)–(vi), (f), (ga), (h); s 7(2)(a), (c).

83 Ibid s 6(1).

84 Ibid s 6C(1).

85 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.20]. The estimate was based on Australian Bureau of Statistics, *Business Growth and Performance Survey, Financial Year 1997/1998* (1999), which has been discontinued since then. There are no further official statistics on the number of Australian small businesses with an annual turnover of $3 million or less. The Australian Bureau of Statistics, however, does publish data on the number of businesses with an annual turnover of less than $2 million. As at June 2007, there are 1,890,213 businesses with an annual turnover of $2 million or less, which represents 94% of all businesses: Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), 20. The small business exemption is discussed in Chapter 39.

86 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 1; N Waters, 'Essential Elements of a New Privacy Act' (1999) 5 *Privacy Law & Policy Reporter* 168, 168.

87 R Clarke, *Flaws in the Glass; Gashes in the Fabric* (1997) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Flaws.html> at 31 March 2008.

88 See, eg, T Dixon, *Government Tables New Privacy Legislation* (2000) AustLII <www.austlii.edu.au/au/other/CyberLRes/2000/6/> at 31 March 2008; Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 3 September 2000; Australian Privacy Charter Council, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry on the Privacy Amendment (Private Sector) Bill 2000*, 20 August 2000.

89 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(4).

commentary or opinion on, or analysis of, these materials.[90] The terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' are not defined. Waters has argued that the lack of definitions and the inclusion of 'information' separately from news, current affairs and documentaries, allow any organisation publishing material to take advantage of the exemption.[91] The exemption that applies in the course of journalism is discussed further in Chapter 42.

33.47 In submissions to this Inquiry, a number of stakeholders suggested that exemptions should be justified and limited to the extent possible;[92] and emphasised the need for a clear rationale for each exemption.[93]

33.48 The Social Security Appeals Tribunal stated that 'agencies should not be excluded from the operation of the *Privacy Act* by genus'.[94] By contrast, the OPC emphasised the need to ensure the consistent coverage of entities that have a similar nature and function, submitting that the consistent application of exemptions would 'foster greater clarity as to the intention and coverage of exemptions'.[95]

33.49 Some stakeholders submitted that it is preferable for exemptions to be targeted at either: specific acts and practices;[96] particular types of information; or specific information handling purposes.[97] One individual suggested that entities should apply for an exemption from the *Privacy Act* on a case-by-case basis, and that any exemption should be limited in time and circumstances.[98] The AFP and the Insurance Council of Australia, on the other hand, submitted that the current exemptions are appropriate.[99]

33.50 The OPC, the Commonwealth Ombudsman and Privacy NSW considered that exempt entities should be encouraged to adopt information-handling standards that are similar to those contained in the *Privacy Act*.[100] Privacy NSW stated that it has formally adopted the Data Protection Principles developed by the New South Wales

---

90 Ibid s 6(1).

91 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149.

92 Commonwealth Ombudsman, *Submission PR 202*, 21 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.

93 Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.

94 Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007.

95 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

96 Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007; SBS, *Submission PR 112*, 15 January 2007.

97 Government of South Australia, *Submission PR 187*, 12 February 2007.

98 K Pospisek, *Submission PR 104*, 15 January 2007.

99 Australian Federal Police, *Submission PR 186*, 9 February 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007.

100 Privacy NSW, *Submission PR 468*, 14 December 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007.

Privacy Committee in 1991 as a best practice standard in dealing with complaints against entities in New South Wales that are not covered by privacy law.[101]

33.51 As noted above, there are more exemptions from the *Privacy Act* than from privacy legislation in other comparable jurisdictions. More importantly, some of the exemptions contained in the *Privacy Act* do not appear to be justified as a matter of public policy, or are framed too broadly. For example, the justification for the exemption that applies to some of the agencies listed under the FOI Act is unclear.[102] One of those exempt agencies, the National Health and Medical Research Council, has acknowledged that it was not aware of the reason for its partial exemption from the operation of the *Privacy Act* and would not object to the removal of the exemption.[103] Similarly, there does not appear to be any sound policy basis for leaving unprotected the personal information contained in employee records.[104]

33.52 Even where an exemption may be justified, sometimes its scope under the existing provisions of the *Privacy Act* is too wide. For instance, media organisations are exempt in relation to activities done 'in the course of journalism', provided that they are publicly committed to certain privacy standards. The term 'journalism' and other key terms, however, are not defined. In addition, 'media organisation' is defined to mean an organisation the activities of which consist of collecting, preparing or disseminating news, current affairs, information or documentary (and related commentary, opinion and analysis) to the public. Arguably, the use of the word 'information' separately from 'news', 'current affairs' and 'documentary', makes the exemption too wide. The lack of criteria for media privacy standards also means that public commitment to *any* privacy statement—even one that has little substance—may allow an individual or organisation to take advantage of the exemption.[105]

33.53 Consistent with international standards, exemptions should be limited to the extent possible and justified on sound policy grounds. The ALRC agrees with the submissions by stakeholders that, even when partial or full exemptions from the *Privacy Act* are justified, the exempt entities should be encouraged to adopt information-handling practices that are, to the extent possible, consistent with the privacy principles. In the remaining chapters in Part E, the ALRC makes a number of recommendations for reform that are intended to give effect to this policy position.

---

101 Privacy NSW, *Submission PR 468,* 14 December 2007. The data protection principles correspond closely to the IPPs in the *Privacy Act 1988* (Cth): Privacy NSW, *Data Protection Principles* <www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_dpps> at 31 March 2008.

102 See Ch 36.

103 National Health and Medical Research Council, *Submission PR 397,* 7 December 2007.

104 See Ch 40.

105 See Ch 42.

Complexity of the exemption provisions

33.54 Some commentators have argued that the exemption provisions in the *Privacy Act* are overly complex.[106] Such complexity sometimes makes it difficult to determine the extent to which individuals and entities are exempt from the Act.

33.55 Certain agencies are, in effect, completely exempt from the operation of the *Privacy Act*—but this may not always be readily apparent from the structure of the provisions. For example, while intelligence agencies fall within the definition of an 'agency', acts done, or practices engaged in, by them are not included in the acts or practices to which the Act generally applies.[107] In addition, s 7(2) of the *Privacy Act* provides that provisions in the Act *except* in respect of the IPPs, the NPPs, an approved privacy code and some of the Privacy Commissioner's functions, *do not* apply to these agencies. This exemption could be simplified by stating clearly that intelligence agencies are completely exempt from the operation of the Act.

33.56 The acts and practices of a number of agencies and organisations initially fall outside the acts or practices to which the Act applies, but the extent of the exemption is then modified either within the same section or through another section. Further, the scope of some exemptions must be ascertained by reference to other legislation.

33.57 For example, one of the schedules to the FOI Act lists a number of agencies that are exempt from the FOI Act in respect of particular documents.[108] These agencies fall within the definition of an 'agency' in the *Privacy Act* and therefore appear to be covered by the Act. Section 7(1)(a)(i) of the Act, however, appears to exempt their acts and practices completely. Section 7(1)(c) then provides that these acts and practices fall within the acts or practices to which the Act applies *except* in relation to records for which the agencies are exempt from the operation of the FOI Act. Further, s 7(2) of the *Privacy Act* provides that the provisions of the Act—except in respect of the IPPs, the NPPs, an approved privacy code and some of the Privacy Commissioner's functions—apply to these agencies. Finally, s 7A provides that, notwithstanding ss 7(1)(a)(i), 7(1)(c) and 7(2), acts and practices done in relation to documents in respect of these agencies' commercial activities, or the commercial activities of another entity, are treated as acts and practices of an organisation.

---

106 T Dixon, 'Preparing for the New Privacy Legislation' (Paper presented at Australia's New Privacy Legislation, Baker & McKenzie Cyberspace Law and Policy Centre CLE Conference, Sydney, 24–25 May 2001); R Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (1989) Australian National University <www.anu.edu.au/people/Roger. Clarke/DV/PActOECD.html> at 14 April 2008.

107 *Privacy Act 1988* (Cth) ss 6(1), 7(1)(a)(i)(B).

108 *Freedom of Information Act 1982* (Cth) sch 2 pt II div 1.

33.58 The ambiguity of some of the exemption provisions also has given rise to criticism.[109] For example, small businesses are defined as businesses with an annual turnover of $3 million or less. It has been argued, however, that it is difficult for customers to know the turnover of a business and, therefore, whether the business is exempt.[110]

33.59 In DP 72, the ALRC noted the comments made by a number of stakeholders concerning the complexity of the exemption provisions in the *Privacy Act*,[111] and the need for a clear statement of the exemptions and their scope.[112] For example, the Legal Aid Commission of New South Wales submitted that that the complexity of the existing exemptions results in uncertainty for individuals seeking remedies under the *Privacy Act*, making it more difficult for legal aid organisations to provide advice.[113]

33.60 Stakeholders expressed particular concern about the complexity of the exemptions provided for in s 7 of the *Privacy Act*.[114] For example, the OPC suggested that s 7 be redrafted because 'it is a very complex and difficult section to understand and apply'—making it difficult for many entities to understand which aspects of their activities are covered by the Act.[115] In contrast, while the ABC acknowledged that the 'carving out and partial reapplication' under s 7 is relatively complex, it suggested that the section does set out the relationship between these exemptions and those applying under the FOI Act.[116]

33.61 ASIO supported the simplification of the exemption provisions that apply to it and other intelligence agencies, provided that this would not alter the scope of the exemption.[117]

---

109 See, eg, Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 3 September 2000; Australian Privacy Charter Council, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry on the Privacy Amendment (Private Sector) Bill 2000*, 20 August 2000.

110 Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005. The small business exemption is discussed further in Ch 39.

111 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Commonwealth Ombudsman, *Submission PR 202*, 21 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; SBS, *Submission PR 112*, 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.

112 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.

113 Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

114 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

115 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

116 Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.

117 Australian Security Intelligence Organisation, *Submission PR 180*, 9 February 2007.

33.62 The ALRC agrees that the exemption provisions are overly complex. In particular, s 7 is very difficult to understand and apply. Simplifying the exemption provisions would assist individuals and entities to understand their rights and obligations under the *Privacy Act*.

33.63 In Chapter 5, the ALRC recommends that the *Privacy Act* be redrafted to achieve greater consistency, simplicity and clarity.[118] This would include the redrafting of the exemption provisions. Specific recommendations for reform also are contained in the following chapters of Part E.

Location of the exemption provisions

33.64 The exemptions from the *Privacy Act* are contained in a number of provisions throughout the Act, including ss 6C–7C, 12A, 12B, 13A–13D and 16E. Setting out these exemptions together in one part of the Act arguably would make the exemption provisions more accessible. For example, exemptions under the FOI Act are set out in a schedule to that Act.

33.65 Some overseas jurisdictions—such as the United Kingdom, New Zealand and Hong Kong—set out most of their exemption provisions in a specific part of the legislation.[119] Other jurisdictions, such as the United States and Canada, group exemption provisions together in one section or consecutive sections.[120]

Submissions and consultations

33.66 In DP 72, the ALRC noted the OPC's submission that a two-pronged approach to locating the exemption provisions should be adopted. Where exemptions exist for certain categories of entities, the exemptions should be grouped together in one part of the Act. Where exemptions exist for specific, named entities, they should be listed in a schedule to the *Privacy Act*. This listing should distinguish between entities with a full exemption and those with a partial exemption.[121]

33.67 The ALRC expressed the preliminary view that, in the interest of accessibility and clarity, the two-pronged approach to locating exemption provisions suggested by the OPC should be adopted. The ALRC therefore proposed that the *Privacy Act* be amended to: group together in a separate Part of the Act exemptions for certain categories of entities or types of acts and practices; and set out in a schedule to the Act

---

118 See Rec 5–2.

119 See, eg, *Data Protection Act 1998* (UK) Part IV—Exemptions; *Privacy Act 1993* (NZ) Part 6—Codes of practice and exemptions from information privacy principles; *Data Protection Act 1988* (Ireland) s 1(4)(c); *Personal Data (Privacy) Ordinance* (Hong Kong) Part VIII—Exemptions.

120 *Privacy Act 1974* 5 USC § 552a (US) (j), (k); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(2).

121 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

exemptions for specific, named entities.[122] The proposed schedule would distinguish between entities that are completely exempt and those that are partially exempt from the *Privacy Act*. For those entities that are partially exempt, the schedule would specify those acts and practices that are exempt.[123]

33.68 Most of the stakeholders who commented on the location of exemption provisions supported the approach proposed in DP 72.[124] There was specific support in submissions for grouping together in a separate part of the Act exemptions for certain categories of entities or types of acts and practices.[125] Stakeholders suggested that this would simplify the Act,[126] make it more accessible,[127] and facilitate compliance by agencies and organisations.[128] Some stakeholders also supported specifically the proposal to set out in a schedule to the *Privacy Act* exemptions for specific, named entities.[129]

33.69 The OVPC and the Australian Privacy Foundation supported the general approach to exemptions proposed in DP 72, but submitted that, in principle, agencies or organisations should not be exempt completely from the obligation to comply with privacy principles.[130]

33.70 The REIA submitted that both exempt entities and those entities specifically made subject to the *Privacy Act* should be listed in subordinate legislation, on the basis that 'regular legislative reviews and changing community concerns are likely to result in ongoing changes to the status of [these] entities'. It stated that this would 'aid the

---

122 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 30–1, 30–2.

123 Ibid, Proposal 30–2.

124 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; Optus, *Submission PR 532*, 21 December 2007 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

125 BPay, *Submission PR 566*, 31 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007s; Australian Taxation Office, *Submission PR 515*, 21 December 2007; P Youngman, *Submission PR 394*, 7 December 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

126 BPay, *Submission PR 566*, 31 January 2008; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

127 BPay, *Submission PR 566*, 31 January 2008; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

128 BPay, *Submission PR 566*, 31 January 2008.

129 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; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. See also Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Confidential, *Submission PR 143*, 24 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.

130 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

modification of the Act over time, in recognition of the need for the *Privacy Act* to stay abreast of technological, social and political developments'.[131]

33.71 It was suggested that, where possible, exemptions should be located within the privacy principles to which they relate, which would avoid misleading impressions of the coverage of the privacy principles and prevent exempt organisations from making claims about their compliance with a principle.[132] Telstra and the ABC, on the other hand, submitted that the exemptions should remain where they are, on the basis that stakeholders are now familiar with the layout of the Act,[133] and the cost of complying with amendments to the *Privacy Act* would outweigh any benefit that would result from a redrafting of the Act.[134]

33.72 Privacy NSW also considered that there was value in placing exemptions within the privacy principles. It submitted that, where an exemption relates to categories of information, it should appear as exceptions to the definition of 'personal information' rather than be linked to the agency or organisation itself.[135]

ALRC's view

33.73 Where exemptions for certain categories of entities or types of acts and practices exist, they should be grouped together in a separate part of the Act. Privacy legislation in some overseas jurisdictions groups exemptions under a separate part of the legislation—for example, Part IV of the *Data Protection Act 1998* (UK) and Part VIII of the *Data Protection (Privacy) Ordinance* (Hong Kong). The categories of entities or types of acts and practices that should be grouped together in a part of the *Privacy Act* include: federal courts; Royal Commissions; the exemption relating to personal use; the journalism exemption; and exemptions applying to related bodies corporate, change in partnership, and an act or practice that is required by foreign law.

33.74 Specific, named entities that are exempt from the *Privacy Act*—such as ASIO; the IGIS; specified federal tribunals, commissions or boards; the ACC and the Integrity Commissioner—should be set out in a schedule to the Act. The schedule should set out clearly the scope of any such exemption. This is consistent with the approach in the FOI Act. In relation to specific agencies that are exempt from both the *Privacy Act* and the FOI Act, such as the Australian Transaction Reports and Analysis Centre, they should be specified in the schedule to the *Privacy Act*, instead of by reference to their

131 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007. See also Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007.
132 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.
133 Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007.
134 Telstra, *Submission PR 185*, 9 February 2007.
135 Privacy NSW, *Submission PR 468*, 14 December 2007.

exempt status under the FOI Act. This would avoid the need to refer to other legislation when determining the exempt status of particular agencies under the *Privacy Act*.

33.75 This two-pronged approach will increase the accessibility and clarity of the exemption provisions. The alternative approach, of locating partial or full exemptions within specific privacy principles, has the potential to render the principles overly complex and unwieldy. Since all of the exemptions relate to specific functions or activities of an agency or organisation, rather than categories of information, locating exemptions within the definition of 'personal information' also would not be appropriate.

Recommendation 33–1 The *Privacy Act* should be amended to group together in a separate part of the Act exemptions for certain categories of agencies, organisations and entities or types of acts and practices.

Recommendation 33–2 The *Privacy Act* should be amended to set out in a schedule to the Act exemptions for specific, named agencies, organisations and entities. The schedule should distinguish between agencies, organisations and entities that are completely exempt and those that are partially exempt from the *Privacy Act.* With respect to partially exempt agencies, organisations and entities, the schedule should specify the particular acts and practices that are exempt.

34. Intelligence and Defence Intelligence Agencies

Contents

Introduction

34.1 The Australian intelligence community comprises six Australian Government agencies: the intelligence agencies—the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Office of National Assessments (ONA); and the defence intelligence agencies—the Defence Intelligence Organisation (DIO), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO). Collectively, these agencies work together to meet Australia's intelligence needs.[1]

34.2 Three of these agencies are responsible for collecting intelligence outside Australia: ASIS is responsible for human intelligence obtained through interaction with people; the DSD for signals intelligence obtained by intercepting electronic

1 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 4.

communications—such as telephones, faxes and emails; and the DIGO for imagery and geospatial intelligence obtained from imaging satellites and other sources.[2]

34.3 The ONA and the DIO are responsible for foreign intelligence assessment. Their functions are to analyse and assess intelligence as well as information from other sources—such as the media, the internet and diplomatic reporting—to form a picture of an issue or occurrence.[3] In this chapter, ASIS, the DIGO, the DSD, the DIO and the ONA—that is, all the intelligence and defence intelligence agencies except ASIO—are collectively referred to as the 'foreign intelligence agencies'.

34.4 ASIO, as a security intelligence agency, focuses mainly on the domestic security of Australia. Unlike the foreign intelligence agencies—which have either an intelligence collection or assessment role but not both—ASIO has both an intelligence collection and an assessment role.[4]

34.5 Currently, the intelligence and defence intelligence agencies are either partially or completely exempt from the *Privacy Act 1988* (Cth). This chapter examines whether they should continue to be exempt.

The defence and defence intelligence agencies

Intelligence agencies

34.6 Under the *Privacy Act*, intelligence agencies are defined to mean ASIO, ASIS and the ONA.[5] Acts and practices of these agencies are completely exempt from the operation of the *Privacy Act*.[6] A record that has originated with, or has been received from, an intelligence agency also is excluded from the operation of the Act.[7] Accordingly, agencies and organisations receiving a record from an intelligence agency are exempt from the operation of the *Privacy Act* in relation to that record. In addition, disclosure of personal information to ASIO or ASIS is not covered by the Act.[8]

34.7 ASIO's main role is to obtain, correlate and evaluate intelligence relevant to security, enabling it to advise the government about risks to national security. It also provides security assessments, gives protective security advice and collects foreign intelligence in Australia.[9] The *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) defines 'security' as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal

2 Ibid, 3.
3 Ibid, 3.
4 Ibid, 3–4.
5 *Privacy Act 1988* (Cth) s 6(1).
6 Ibid s 7(1)(a)(i)(B), (2)(a).
7 Ibid s 7(1)(f).
8 Ibid s 7(1A)(a), (b).
9 *Australian Security Intelligence Organisation Act 1979* (Cth) s 17.

violence, attacks on Australia's defence system and acts of foreign interference; and the carrying out of Australia's responsibilities to any foreign country in relation to these matters.[10] ASIO falls within the portfolio responsibilities of the Attorney-General.

34.8 ASIS is Australia's overseas intelligence collection agency. Its role is to collect and distribute foreign intelligence that may impact on Australian interests, undertake counter-intelligence activities and liaise with overseas intelligence and security agencies.[11] ASIS is responsible to the Australian Government through the Minister for Foreign Affairs.[12] Under the *Intelligence Services Act 2001* (Cth), the Director-General of ASIS is directly responsible to the Minister.[13]

34.9 The ONA was established by the *Office of National Assessments Act 1977* (Cth) as an independent agency accountable to the Prime Minister. It produces assessments and reports on international political, strategic and economic matters in order to assist the Prime Minister, ministers and departments in the formation of policy and plans. The ONA also coordinates Australia's foreign intelligence activities and matters of common interest to the foreign intelligence agencies. In addition, the ONA is responsible for evaluating Australia's foreign intelligence activities and providing advice on the adequacy of resources available for such activities.[14] The Director-General of the ONA is an independent statutory office holder, and as such is not subject to external direction on the content of assessments by the ONA.[15]

Defence intelligence agencies

34.10 The Defence Intelligence Group in the Department of Defence consists of three units: the DSD, the DIGO and the DIO. They are exempt from the operation of the *Privacy Act* where their acts and practices relate to their activities.[16] Records that have originated with, or have been received from, these agencies also are excluded from the operation of the Act.[17] Accordingly, agencies and organisations receiving a record from these agencies are exempt from the operation of the *Privacy Act* in relation to that

10 Ibid s 4.
11 *Intelligence Services Act 2001* (Cth) s 6(1); Australian Secret Intelligence Service, *What We Do* <www.asis.gov.au/what.html> at 7 April 2008.
12 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 10.
13 *Intelligence Services Act 2001* (Cth) s 18(2).
14 *Office of National Assessments Act 1977* (Cth) s 5; Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 7 April 2008.
15 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 8.
16 *Privacy Act 1988* (Cth) s 7(1)(ca).
17 Ibid s 7(1)(g).

record. Furthermore, disclosure of personal information to the DSD is not covered by the Act.[18]

34.11 The functions of the DSD and the DIGO, and certain limits on their activities, are set out in the *Intelligence Services Act*. The DSD is the national authority on security of information on communications and information systems across government. Its principal functions are to collect and communicate foreign signals intelligence, and provide advice to the Australian Government on the security and integrity of information processed, stored or communicated in electronic form.[19]

34.12 The DIGO provides intelligence information derived from imagery and other sources in support of Australia's defence and national interests.[20] It is responsible for obtaining and communicating imagery and geospatial intelligence to help meet Australia's foreign intelligence requirements, supporting the operations of the Australian Defence Force, and supporting the national security and emergency response functions of federal, state and territory authorities.[21]

34.13 The DIO analyses foreign developments and provides intelligence assessments to support the Department of Defence, the planning and conduct of defence force operations, and wider government decision making. It is responsible for assessing military intelligence relating to global security trends, weapons of mass destruction, terrorism, military capabilities, defence economics, and science and technology with military applications.[22] There is no legislation specific to the DIO, although some of its activities are covered under the *Intelligence Services Act*.[23]

Rationale for the exemption of the intelligence and defence intelligence agencies

34.14 The Inspector-General of Intelligence and Security (IGIS), the main body charged with oversight of the intelligence and defence intelligence agencies, has stated that one of the reasons why the Australian intelligence agencies should be exempt, or partially exempt, from the provisions of the *Privacy Act* is that 'it is necessary for the agencies to protect their sources, capabilities and methods if they are to function

---

18 Ibid s 7(1A)(c).

19 *Intelligence Services Act 2001* (Cth) s 7.

20 Australian Government Department of Defence, *Defence Imagery and Geospatial Organisation—About DIGO* <www.defence.gov.au/DIGO/About_Us/about.html> at 7 April 2008.

21 *Intelligence Services Act 2001* (Cth) s 6B; Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 11.

22 Australian Government Department of Defence, *Defence Intelligence Organisation* <www.defence.gov.au/dio> at 7 April 2008; Australian Government Department of Defence, *Defence Intelligence Organisation—FAQs* <www.defence.gov.au/dio/faq.html> at 7 April 2008.

23 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 5.

effectively'.[24] Other reasons for the exemption include that: there already are adequate privacy requirements applying to the intelligence and defence intelligence agencies contained in legislation, ministerial directions and guidelines; there are robust accountability and oversight mechanisms applying to the agencies; and the exemption is consistent with international standards. These reasons are discussed below.

Privacy requirements

Legislation

34.15 Intelligence and defence intelligence agencies only may collect intelligence on Australians under warrant or authorisation by a responsible minister. As discussed below, the *Intelligence Services Act* sets out the circumstances in which the responsible minister may authorise intelligence activity by the ASIS, the DIGO or the DSD against an Australian person.

34.16 Section 8 of the *Intelligence Services Act* provides that the responsible minister must issue a direction requiring ASIS, the DIGO or the DSD to obtain an authorisation under s 9 from the minister before undertaking intelligence activity on an Australian person. Section 32B of the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act) requires the minister to give a copy of any such direction to the IGIS as soon as practicable after it is given. The validity of a ministerial authorisation given under s 9 is limited to no more than six months, and may be renewed only if the relevant minister is satisfied that it is necessary for the authorisation to continue to have effect.[25] A copy of the authorisation must be kept by the agency and made available for inspection on request by the IGIS.[26]

34.17 The agency heads of ASIS, the DIGO and the DSD must give to the responsible minister a written report in respect of intelligence activities carried out by the agency in reliance on a ministerial authorisation. The report must be provided to the minister within three months from the day on which the authorisation ceased to have effect.[27]

34.18 The *Intelligence Services Act* also sets out limits on the functions of ASIS, the DIGO and the DSD. The functions are only to be performed in the interests of Australia's national security, foreign relations and national economic well-being, and 'to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia'.[28] These three agencies are prohibited

---

24 Inspector-General of Intelligence and Security, 'Trust and the Rule of Law' (Paper presented at Australian Institute of Professional Intelligence Officers, Intelligence 2005 Conference, 3 November 2005), 4.

25 *Intelligence Services Act 2001* (Cth) ss 9(4), 10.

26 Ibid s 9(5).

27 Ibid s 10A.

28 Ibid s 11.

from undertaking any activity that is unnecessary for the proper performance of their functions, or not authorised or required by or under another Act.[29]

34.19 Generally, ASIO may collect information relevant to security under warrant.[30] In addition, only the Director-General of Security, or an ASIO officer authorised by the Director-General, can communicate intelligence on behalf of ASIO. It is an offence for an ASIO employee or agent to convey information acquired in the course of his or her duties outside ASIO without the authority of the Director-General of Security. The Director-General of Security may authorise an ASIO officer to communicate information to authorities of any other country approved by the Director-General.[31] Section 20 of the ASIO Act places a special responsibility upon the Director-General of Security to take all reasonable steps to ensure that the work of ASIO is limited to what is necessary for the purposes of the discharge of ASIO's functions.

Attorney-General's guidelines issued under the Australian Security Intelligence Organisation Act 1979 (Cth)

34.20 Under s 8A of the ASIO Act, the Attorney-General may give the Director-General of Security guidelines to be observed by ASIO in the performance of its functions or the exercise of its powers. In 1992, the then Attorney-General issued two separate guidelines concerning the performance by ASIO of its functions relating to obtaining intelligence relevant to security and politically motivated violence.[32] These guidelines have been revised in late 2007 and combined into a single set of guidelines (Attorney-General's Guidelines).[33] The Attorney-General's Guidelines contain general guidance on obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence), as well as specific guidance on the treatment of personal information.

34.21 In terms of general guidance, the Attorney-General's Guidelines specify the purposes for which ASIO may collect, maintain, analyse and assess information relevant to security, and the types of information that may be collected.[34] The Director-

---

29 Ibid s 12.

30 *Australian Security Intelligence Organisation Act 1979* (Cth) pt III divs 2 and 3. The only exception is where an authorised ASIO officer or employee requests information or documents from an operator of an aircraft or vessel relating to its cargo, crew, passenger, stores or voyages: *Australian Security Intelligence Organisation Act 1979* (Cth) s 23.

31 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18–19.

32 See Australian Government Inspector-General of Intelligence and Security, *Annual Report 2006–2007* (2007), 39.

33 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Function of Obtaining, Correlating, Evaluating and Communicating Intelligence relevant to Security (including Politically Motivated Violence)* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 7 April 2008. See also N O'Brien, 'Changes Permit ASIO to Keep Files', *The Australian* (online), 13 October 2007, <www.theaustralian.news.com.au>.

34 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Function of Obtaining, Correlating, Evaluating and Communicating Intelligence relevant to Security (including Politically*

General of Security is required to establish processes to ensure that all requests for information from external agencies are authorised at an appropriate level.[35] In conducting its inquiries and investigations, ASIO must obtain information in a lawful, timely and efficient way.[36] The means of obtaining information must be proportionate to the gravity of the threat and the probability of its occurrence, and inquiries and investigations should be conducted 'using as little intrusion into individual privacy as possible'.[37] The least intrusive techniques of information collection should be used whenever possible.[38] A greater degree of intrusion may be justified, however, where a threat is assessed as likely to develop quickly; or where there is a threat of politically motivated violence against specified persons or classes of persons, such as internationally protected persons.[39] The seniority of the officer required to approve an investigative technique should increase with the level of intrusiveness of the technique.[40]

34.22 Guideline 13 of the Attorney-General's Guidelines specifically deals with the collection, use and disclosure of personal information, as well as data quality and data security. It requires that ASIO only collect, use, handle or disclose personal information for purposes connected with its statutory functions.[41] The Director-General is required to:

- take all reasonable steps to ensure that ASIO does not collect, use, handle or disclose personal information unless it is reasonably necessary for the performance of its statutory functions;

- ensure that all reasonable steps are taken to ensure that the personal information held, used or disclosed by ASIO is accurate and not misleading; and

- ensure that all personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification.[42]

34.23 The Attorney-General's Guidelines also contain record-keeping requirements on all requests for personal information by ASIO, all personal information received in response to such requests, and all communication by ASIO of personal information for

---

Motivated Violence) <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 7 April 2008, Guidelines 6.2, 10.3.

35 Ibid, Guideline 8.2.

36 Ibid, Guideline 10.4.

37 Ibid, Guideline 10.4(a), (b).

38 Ibid, Guidelines 10.4(d).

39 Ibid, Guidelines 10.4(e), 15.12.

40 Ibid, Guidelines 10.4(c).

41 Ibid, Guideline 10.1.

42 Ibid, Guidelines 13.2, 13.3, 13.6.

purposes relevant to security or as otherwise authorised. These records must be open to inspection by the IGIS.[43] In addition, the Attorney-General's Guidelines state that, where an inquiry or investigation concludes that a subject's activities are not, or are no longer, relevant to security, the relevant records are to be destroyed pursuant to disposal schedules agreed to between ASIO and the National Archives of Australia.[44]

34.24 The IGIS has oversight responsibility to ensure that ASIO complies with the Attorney-General's Guidelines in conducting its activities. During 2006–07, the IGIS reported that his office inspected records associated with a wide range of ASIO activities, including warrant operations, approvals to commence an investigation, and reviews of investigations. The IGIS stated that the quality of the requests for warrant made to the Attorney-General have been 'of a consistently high standard'. The IGIS also reported his overall satisfaction with ASIO's adherence to the Attorney-General's Guidelines in relation to the obtaining and review of approvals to investigate. He noted several instances of 'minor procedural defects' during the reporting period, but did not consider that there were any systemic concerns.[45]

Privacy rules issued under the Intelligence Services Act 2001 (Cth)

34.25 Under s 15 of the *Intelligence Services Act*, the responsible minister is required to make written rules regulating the communication and retention by the DIGO, the DSD and ASIS of intelligence information concerning Australians. Before making the rules, the responsible minister must consult with the head of the relevant agency as well as the IGIS and the Attorney-General.

34.26 The current privacy rules for ASIS, the DSD and the DIGO are broadly consistent with each other.[46] The rules provide for the circumstances in which the agency may communicate and retain intelligence information concerning an Australian person. In addition, they provide that where the agency has communicated intelligence information concerning an Australian person contrary to the rules, or because it had presumed wrongly that a person was not an Australian person, the agency shall immediately consult with or inform the IGIS of the measures taken to protect the privacy of the Australian person.[47] The rules, however, do not require the agency to observe particular standards when engaging in other information-handling practices

---

43 Ibid, Guidelines 13.4, 13.5.

44 Ibid, Guideline 11.2.

45 See Australian Government Inspector-General of Intelligence and Security, *Annual Report 2006–2007* (2007), 42, 45–46. Note that the IGIS's assessment relates to ASIO's compliance with the 1992 privacy guidelines issued by the Attorney-General to the Director-General of Security: see Australian Government Inspector-General of Intelligence and Security, *Annual Report 2006–2007* (2007), 39.

46 R Hill, *Defence Imagery and Geospatial Organisation Privacy Rules* (2005) Australian Government Department of Defence <www.defence.gov.au/DIGO/About_Us/about.html> at 10 April 2008; P Reith, *Defence Signals Directorate: Privacy Safeguards* (2001) Australian Government Defence Signals Directorate <www.dsd.gov.au/about_dsd/privacy_safeguards.html> at 10 April 2008; A Downer, *Australian Secret Intelligence Service: Rules to Protect the Privacy of Australians* (2001) Australian Secret Intelligence Service <www.asis.gov.au/privacygov.html> at 10 April 2008.

47 R Hill, *Defence Imagery and Geospatial Organisation Privacy Rules* (2005) Australian Government Department of Defence <www.defence.gov.au/DIGO/About_Us/about.html> at 10 April 2008, r 6.

that are dealt with in the Information Privacy Principles (IPPs), such as accuracy, storage and security of personal information.

34.27 In his annual report for 2006–07, the IGIS stated that his office undertook on-going monitoring of ASIS's compliance with privacy rules. He also reviewed regularly reports containing secret intelligence information to ensure that the information was handled in accordance with the requirements of the *Intelligence Service Act* and the privacy rules. The IGIS reported that that he has 'seen no privacy abuses in the material we have access to, and that there is a commitment within ASIS to the rigorous application of the privacy rules'.[48]

34.28 In relation to the DSD, the IGIS reported that a fully-staffed section within the DSD monitors the DSD's compliance with the privacy rules, and his office fulfils a similar function independently of the DSD. He stated that there was a regular dialogue between the DSD and his office on privacy issues, and that he was satisfied that the incidence of Australian persons being identified in DSD's reporting was extremely low relative to the number of reports DSD disseminated. In addition, the IGIS stated that notwithstanding the highly intrusive nature of DSD's work, privacy issues were taken very seriously by the DSD.[49]

34.29 During 2006–07, the IGIS visited DIGO headquarters every two months and 'closely examined all tasking requests DIGO receives which might impact upon Australian persons or interests, for compliance with the DIGO's privacy rules'. He commented that, while a uniform approach to the handling of privacy-related matters by foreign intelligence collection agencies is commendable, it presented certain challenges for DIGO due to DIGO's predominantly image-based reporting on property or premises that may fall within the definition of an 'Australian person'. The IGIS stated, however, that 'the vast majority of DIGO's reporting has an off-shore focus, and that the privacy rules come into play relatively infrequently'. The IGIS was satisfied that the DIGO was committed to applying the privacy rules, and that it 'was inclined to take a cautious and conservative approach rather than to disregard the requirements of the rules'.[50]

Administrative privacy guidelines

34.30 Unlike ASIS, the DSD and the DIGO, the ONA and the DIO are not required by legislation to have privacy rules or guidelines in place. A review of the *Intelligence Services Act* in 2005–06 coordinated by the Department of the Prime Minister and Cabinet resulted in a government decision that the ONA and the DIO should be subject to privacy guidelines consistent with the requirements placed on ASIS, the DSD and

48 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2006–2007* (2007), 57.
49 Ibid, 62.
50 Ibid, 65.

the DIGO. The ONA and the DIO have since developed and implemented privacy guidelines that are broadly consistent with those in use elsewhere by other intelligence and defence intelligence agencies. The IGIS was consulted by the ONA and the DIO in the development of the guidelines.[51] Both sets of guidelines have been in effect since December 2005.[52]

34.31 The purpose of the guidelines is to ensure that in the agencies' external communications, the privacy of Australians is preserved as far as is consistent with the proper performance of the agencies' functions.[53] The guidelines for the ONA and the DIO constitute a direction to all agency staff by the responsible minister.[54] Copies of the guidelines are annexed to the IGIS's Annual Report for 2005–06, and the ONA's privacy guidelines also are available on its website.[55]

34.32 During the reporting period 2006–07, the IGIS conducted five inspections of the ONA and another five of the DIO to ascertain the extent of compliance with the guidelines. The IGIS was generally satisfied with the quality of the documentation and the thorough implementation of the guidelines at both the DIO and the ONA. The IGIS also reported that the DIO and the ONA have continued to educate analysts on how to apply, and report on compliance with, the guidelines. In the most recent Annual Report, the IGIS stated that he intended to continue to conduct inspections of the DIO and the ONA every three months to monitor compliance with the guidelines.[56]

Protective Security Manual

34.33 In addition to privacy rules and guidelines that apply to individual agencies, all the intelligence and defence intelligence agencies are required to comply with the *Protective Security Manual*. The *Protective Security Manual* is a policy document produced, and periodically revised, by the Attorney-General's Department (AGD) on behalf of the Protective Security Policy Committee.

> It is the principal means for disseminating Australian Government protective security policies, principles, standards and procedures, to be followed by all Australian Government agencies for the protection of official resources.[57]

34.34 The *Protective Security Manual* sets out guidelines and minimum standards relating to protective security for Australian Government agencies and officers, as well as for contractors and their employees who perform services for the Australian

---

51 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2005–2006* (2006), 50–51, 53–54.

52 Ibid, 8.

53 Ibid, Annex 6 (DIO), Annex 7 (ONA).

54 Ibid, 8.

55 Ibid, Annex 6 (DIO), Annex 7 (ONA). The Australian Government Inspector-General of Intelligence and Security, *Annual Report 2005–2006* (2006) is available on the IGIS's website <www.igis.gov.au>.

56 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2006–2007* (2007), 67, 70.

57 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 8 April 2008.

Government. Of particular relevance is Part C of the *Protective Security Manual*, which provides 'guidance on the classification system and the protective standards required to protect both electronic and paper-based security classified information'.[58] This part sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information.

34.35 Although the *Protective Security Manual*—as it applies to the intelligence and defence intelligence agencies—addresses some of the privacy issues that are not dealt with under these agencies' privacy rules or guidelines, the privacy protections under the *Protective Security Manual* guidelines are restricted to security classified information. Other matters under the IPPs, such as the accuracy of personal information, are not dealt with.

34.36 The intelligence and defence intelligence agencies also are required to comply with the *Australian Government Information and Communications Technology Security Manual* (ACSI 33), which provides guidance to Australian Government agencies on the protection of their information and communication technology systems.[59]

34.37 In its report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC recommended that a revised *Protective Security Manual* be placed in the public domain, with any sensitive security information removed.[60] In September 2005, the AGD released a revised *Protective Security Manual*. The availability of the manual, however, remains restricted to Australian Government agencies. The ALRC continues to be of the view that the *Protective Security Manual* should be a publicly available document, as recommended in ALRC 98.

Secrecy provisions

34.38 Sections 39, 39A and 40 of the *Intelligence Services Act* prohibit the communication of any information or matter that was prepared by or on behalf of ASIS, the DIGO or the DSD in connection with their functions. These provisions apply to a person who: is a current or former staff member of ASIS, the DIGO or the DSD; has entered into a contract, agreement or arrangement with one of these agencies; or has been an employee or agent of a person who has entered into a contract, agreement or arrangement with one of these agencies.

---

58 Ibid.

59 Australian Government Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual (ACSI 33)* (2007).

60 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 4–1.

34.39 Similarly, it is an offence for an ASIO employee or agent to convey information acquired in the course of his or her duties outside ASIO without the authority of the Director-General of Security.[61]

Accountability and oversight mechanisms

34.40 Whether intelligence and defence intelligence agencies should continue to be exempt from the operation of the *Privacy Act* depends, in part, on whether current accountability principles and oversight mechanisms adequately address privacy issues.

Inspector-General of Intelligence and Security

34.41 The IGIS is an independent statutory officer who is responsible for ensuring that the intelligence and defence intelligence agencies 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. To ensure the independence of the office, the IGIS is appointed by the Governor-General for a fixed term of five years and can be dismissed only on limited grounds.[62] An IGIS cannot be appointed more than twice.[63]

34.42 The IGIS conducts inquiries, investigates complaints, makes recommendations to government and provides annual reports to the Australian Parliament. Sections 8 and 11 of the IGIS Act allow the IGIS to undertake inquiries in response to a complaint, at the request of the responsible minister or on the IGIS's own initiative, into a number of matters relating to the operations of the intelligence and defence intelligence agencies—including their compliance with the law, ministerial directions and guidelines, propriety and human rights standards.[64] The IGIS is directly accountable to the Prime Minister.

34.43 When exercising its inquiry function, the IGIS has significant powers that are similar to those of a Royal Commission. The IGIS has powers to obtain information, require persons to answer questions and produce documents, take sworn evidence and enter the premises of any intelligence or defence intelligence agency.[65] Under s 20 of the IGIS Act, the IGIS may obtain documents with a national security classification for the purposes of an inquiry. The IGIS must make arrangements with the head of the relevant agency for the protection of those documents while they remain in the IGIS's possession, and for their return.

34.44 The IGIS has conducted several inquiries into the activities of intelligence and defence intelligence agencies, including inquiries into: intelligence activities in relation to the Tampa incident; terrorist attacks in Bali in October 2002; allegations that the

---

61 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18.
62 *Inspector-General of Intelligence and Security Act 1986* (Cth) ss 6(2), 26, 30.
63 Ibid s 26(2).
64 Ibid ss 8, 11.
65 Ibid ss 18–20.

DSD intercepted communications of the Hon Laurie Brereton MP; and concerns raised about the DIO by Lieutenant Colonel Lance Collins.[66]

Ministerial oversight

34.45 The heads of the intelligence and defence intelligence agencies are responsible to their respective ministers in accordance with normal governance arrangements. The IGIS also assists ministers in their oversight of the intelligence and defence intelligence agencies by conducting inquiries into the agencies at the request of the ministers.[67]

34.46 In addition, the intelligence and defence intelligence agencies are guided by the National Security Committee, which sets broad policy and priorities for the agencies. The Committee is supported by the Secretaries Committee on National Security (SCNS), a committee of senior officials chaired by the Secretary of the Department of the Prime Minister and Cabinet and attended by the secretaries of the National Security Committee's portfolio departments, the Director-General of the ONA and the Director-General of Security. The SCNS advises the National Security Committee on national security policy, coordinates implementation of policies and programs relevant to national security, and guides departments and agencies involved in intelligence and security.[68]

Parliamentary oversight

34.47 Under s 29 of the *Intelligence Services Act*, the oversight responsibilities of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) include:

- reviewing the administration and expenditure of intelligence and defence intelligence agencies;

---

66 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2001–2002* (2002), Annex 2; Australian Government Inspector-General of Intelligence and Security, *Annual Report 2002–2003* (2003), Annex 2, 3; Australian Government Inspector-General of Intelligence and Security, *Annual Report 2003–2004* (2004), Annex 3, 4. See also Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 15. On 6 December 2000, Lieutenant Colonel Lance Collins of the Australian Defence Force wrote to the Minister for Defence expressing concerns that: the DIO acted in mid-1998 to quash early warning, included in an assessment prepared by him, of problems developing in East Timor; the DIO's assessments concerning East Timor were pro-Indonesia; and the DIO cut access to an intelligence database without warning. The IGIS was asked by the Minister for Defence to investigate, report and make recommendations about Collins' allegations. The IGIS found that Collins' view was sincerely held but unfounded: Australian Government Inspector-General of Intelligence and Security, *Annual Report 2003–2004* (2004), Annex 3.

67 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 13.

68 Ibid, 14.

- reviewing any matter in relation to the intelligence and defence intelligence agencies referred to the Committee by the responsible minister or a resolution of either House of the Parliament; and

- reporting the Committee's comments and recommendations to each House of the Parliament and to the responsible minister.[69]

34.48 The intelligence and defence intelligence agencies also are subject to scrutiny by Senate legislation committees in respect of their finance and administration, particularly their budget allocations. In addition, the IGIS is accountable to the Senate Finance and Public Administration Committee.[70]

34.49 ASIO produces an unclassified annual report for tabling in Parliament. It also provides a classified annual report to the Attorney-General, the Prime Minister and the Leader of the Opposition on its activities.[71] In the annual reports of the Department of Defence and the IGIS, broad references are made to the activities of the DIGO, DSD and the DIO. The heads of ASIS and the ONA must provide the responsible minister with a report on their operations at least annually.[72] Although these annual reports are not made public, both ASIS and the ONA also produce unclassified budget documents.[73]

Royal Commissions and other inquiries

34.50 The intelligence and defence intelligence agencies have been the subject of several Royal Commissions and a number of other inquiries. The Hon Justice Robert Hope conducted two Royal Commissions into these agencies during the 1970s and 1980s, which broadly established their current structure, functions and processes.[74] In March 1995, the Hon Gordon Samuels QC and Michael Codd concluded a Royal Commission that inquired into the effectiveness of ASIS's organisation, management, control and accountability arrangements, protection of sources and resolution of grievances and complaints.[75]

---

69 The Committee also has responsibilities for reviewing the operation, effectiveness and implications of certain amendments to anti-terrorism legislation; and ASIO's questioning and detention powers under Division 3 of Part III of the ASIO Act: *Intelligence Services Act 2001* (Cth) s 29(1)(ba), (bb).

70 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 14.

71 *Australian Security Intelligence Organisation Act 1979* (Cth) s 94.

72 *Intelligence Services Act 2001* (Cth) s 42; *Office of National Assessments Act 1977* (Cth) s 19.

73 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 15.

74 See P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet, 4.

75 Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service (Public Edition)* (1995).

34.51 The Parliamentary Joint Committee on ASIO, ASIS and DSD (now the PJCIS) conducted a number of inquiries into intelligence issues, including: an inquiry into the intelligence on Iraqi's weapons of mass destruction;[76] reviews of intelligence services legislation;[77] assessments of the government's proposed amendment of the ASIO Act;[78] and an examination of the nature, scope and appropriateness of ASIO's public reporting activities.[79]

34.52 In 2004, the then Prime Minister appointed Mr Philip Flood AO to conduct an inquiry into the effectiveness of the intelligence community's current oversight and accountability mechanisms, and the delivery of high quality and independent intelligence advice to the government. In the 2004 *Report of the Inquiry into Australian Intelligence Agencies* (Flood Report),[80] it was acknowledged that all elements of government, including the AIC, should be accountable. The Report stated, however, that different accountability and oversight mechanisms for intelligence agencies are justified because of the need for parts of the intelligence function to remain secret. The Flood Report stated that purpose-specific institutions and systems are needed to deal with the tension between accountability and secrecy.[81] The Report found that accountability arrangements for the intelligence agencies were working effectively and that the *Intelligence Services Act* has worked well in practice.[82]

34.53 The Flood Report, however, did recommend some changes to the accountability arrangements relating to the intelligence and defence intelligence agencies, including that: the mandate of the Parliamentary Joint Committee on ASIO, ASIS and DSD (now the PJCIS) be extended to cover all of the relevant agencies; the functions and ministerial accountabilities of the DIGO be formalised in legislation by amendments to the *Intelligence Services Act*; and the mandate of the IGIS be extended to allow the

---

76 Parliament of Australia—Parliamentary Joint Committee on ASIO, ASIS and DSD, *Intelligence on Iraq's Weapons of Mass Destruction* (2003).

77 Parliament of Australia—Joint Select Committee on the Intelligence Services, *An Advisory Report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and Certain Parts of the Cybercrime Bill 2001* (2001); Parliament of Australia—Parliamentary Joint Committee on ASIO, ASIS and DSD, *Review of the Intelligence Services Amendment Bill 2003* (2004); Parliament of Australia—Parliamentary Joint Committee on ASIO, ASIS and DSD, *Review of the Intelligence Services Legislation Amendment Bill 2005* (2005).

78 Parliament of Australia—Parliamentary Joint Committee on the Australian Security Intelligence Organization, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999* (1999); Parliament of Australia—Parliamentary Joint Committee on ASIO, ASIS and DSD, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002* (2002).

79 Parliament of Australia—Joint Select Committee on the Intelligence Services, *A Watching Brief: The Nature, Scope and Appropriateness of ASIO's Public Reporting Activities* (2000).

80 P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet.

81 Ibid, 51.

82 Ibid, 57.

IGIS to initiate inquiries into matters relating to the ONA and the DIO without ministerial referral.[83] All of these recommendations have been implemented.

34.54 In *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), the ALRC and the Administrative Review Council (ARC) also were of the view that scrutiny by the IGIS and the Parliamentary Committee on ASIO of the internal processes and methods of intelligence agencies is adequate.[84] They therefore recommended that intelligence agencies remain exempt from the operation of the *Freedom of Information Act*.[85]

Commonwealth Ombudsman

34.55 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.[86] The Act also permits the Ombudsman, in some circumstances, to decline to investigate; for example, where a matter has not yet been put to the relevant agency.[87] The *Ombudsman Act* enables the Ombudsman to report in a number of ways following an investigation, although it requires the investigation itself to be conducted in private and with fairness to anyone likely to be criticised.[88] The disclosure of identifying information about a complainant is prohibited unless the disclosure is fair and reasonable in all the circumstances.[89]

34.56 The AGD and the Departments of Defence, Foreign Affairs and Trade, and the Prime Minister and Cabinet are within the Ombudsman's jurisdiction.[90] ASIO and the IGIS, however, are excluded.[91] ASIS, the ONA, the DSD, the DIO and the DIGO fall within the Ombudsman's jurisdiction but, in practice, people seeking to make complaints about them are referred to the IGIS.[92] The Ombudsman also is appointed as the Defence Force Ombudsman under the *Ombudsman Act*.[93]

34.57 The Act provides the Ombudsman with an extensive range of powers to investigate, including a power to require the production of information or documents.[94] This power is limited, however, by s 9(3), which provides that the Attorney-General

---

83 Ibid, 59–60.
84 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [11.13].
85 Ibid, Rec 74.
86 *Ombudsman Act 1976* (Cth) s 5.
87 Ibid s 6.
88 Ibid ss 15–17, 19, 35A(3)(a), 35A(3E)(a).
89 Ibid ss 8(2), 35A(3)(b), 35A(3E)(b).
90 Ibid s 5(1)(a).
91 *Ombudsman Regulations 1977* (Cth) regs 4, 6.
92 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [2.43].
93 *Ombudsman Act 1976* (Cth) s 19B.
94 Ibid s 4.

may issue a certificate certifying that the disclosure to the Ombudsman of certain information or documents would be contrary to the public interest for a number of reasons—including that it would prejudice the security, defence or international relations of the Australian Government.

Security Appeals Division of the Administrative Appeals Tribunal

34.58 The Security Appeals Division of the Administrative Appeals Tribunal (AAT) deals with three types of matters, namely, applications for review of: adverse or qualified security assessments made by ASIO; decisions of the National Archives of Australia in respect of access to a record of ASIO; and preventative detention orders issued or extended under the *Criminal Code*.[95] The AAT, however, does not have power to review security assessments conducted by agencies other than ASIO.

34.59 Under the ASIO Act, a security assessment cannot be made in respect of a person who is not: an Australian citizen; the holder of a valid permanent visa; or the holder of a special category or special purpose visa.[96] During review by the AAT, the Director-General of Security is required to present to the AAT all relevant information available to the Director-General, whether favourable or unfavourable to the applicant. The applicant and his or her representative may be present when the AAT is hearing submissions made or evidence adduced by the Director-General of Security or the Australian Government agency to which the assessment was given—unless the minister administering the ASIO Act certifies that disclosure of the evidence or submissions would be contrary to the public interest because it would prejudice security or the defence of Australia.[97]

Australian National Audit Office

34.60 The Australian National Audit Office (ANAO) is a specialist public sector agency responsible for auditing the activities of most Australian Government public sector entities.[98] The Auditor-General has broad information-gathering powers and authority to access Australian Government premises.[99] The scope of its audit program includes all of the intelligence and defence intelligence agencies.[100] The ANAO undertakes annual audits of the financial statements of ASIO, ASIS and the ONA; audits of the Department of Defence that include a consideration of the financial operations of the DIO, the DSD and the DIGO; and occasional performance audits of

---

95 *Administrative Appeals Tribunal Act 1975* (Cth) s 19(6); *Australian Security Intelligence Organisation Act 1979* (Cth) s 54; *Criminal Code Act 1995* (Cth) s 105.51(6). See also G Downes, 'The Security Appeals Division of the Administrative Appeals Tribunal—Functions, Powers And Procedures' (Paper presented at National Security Law Course, University of Sydney, Sydney, 13 September 2006), 6.

96 *Australian Security Intelligence Organisation Act 1979* (Cth) s 36.

97 *Administrative Appeals Tribunal Act 1975* (Cth) s 39A(3), (6), (8), (9).

98 *Auditor-General Act 1997* (Cth) s 39 and pt 4.

99 Ibid pt 5 div 1.

100 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 16.

programs relevant to the intelligence and defence intelligence agencies, usually as part of a wider cross-government consideration of security issues.[101]

Opposition briefing

34.61 Section 21 of the ASIO Act requires that the Director-General of Security brief the Leader of the Opposition for the purpose of keeping him or her informed on matters relating to security. Similarly, the Director-General of ASIS must consult regularly with the Leader of the Opposition in the House of Representatives for the purpose of keeping him or her informed on matters relating to ASIS.[102]

International instruments

34.62 A number of international instruments recognise the need to balance the interests of national security and defence with the interests of privacy or data protection. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, issued by the Organisation for Economic Co-operation and Development (OECD Guidelines), provide that acceptable bases for exceptions in the Guidelines include national sovereignty and national security.[103]

34.63 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive), issued by the European Parliament, contains exemptions concerning public security, defence and state security.[104]

34.64 Similarly, the *Asia-Pacific Economic Cooperation Privacy Framework* (APEC Privacy Framework) states that it is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy interests. It does provide, however, that exceptions to the principles—including those relating to national sovereignty, national security, public safety and public policy—should be limited and proportional to meeting the objectives to which the exceptions relate. They should also be and made known to the public; or should be in accordance with law.[105]

Discussion Paper proposal

34.65 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC considered whether the intelligence and defence intelligence agencies should continue to be exempt from the operation of the *Privacy Act*. The ALRC noted that a number of

---

101 P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet, 57.

102 *Intelligence Services Act 2001* (Cth) s 19.

103 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 4; Memorandum, [46].

104 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), arts 3(2), 13; recitals 16, 43.

105 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

stakeholders considered the current exemption to be appropriate,[106] provided that there was sufficient oversight.[107] Submissions from the Office of the Privacy Commissioner (OPC) and the intelligence and defence intelligence agencies supported the view that some of the IPPs were incompatible with the functions of the intelligence and defence intelligence agencies.[108] The foreign intelligence agencies—ASIS, the ONA, the DSD, the DIO and the DIGO—stated that the collection and communication[109] of personal information is a central part of their intelligence function.[110] Both the foreign intelligence agencies and ASIO were concerned that a requirement that they comply with the provisions of the *Privacy Act* would constrain unduly their ability to carry out their functions. Such a requirement, they argued, could:

- prejudice their methods of intelligence collection;[111]
- disclose their methods, capabilities and sources to persons of security interest;[112]
- alert such persons to the fact and scope of the agency's covert investigations;[113]
- enable persons of security interest to adopt defensive security measures that would hinder intelligence collection;[114] and
- undermine their domestic and international liaison relationships, because partner agencies would be likely to withhold the sharing of intelligence where there is a requirement for the relevant intelligence or defence intelligence agency to disclose this information to persons of security interest.[115]

---

106 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Security Intelligence Organisation, *Submission PR 180*, 9 February 2007; Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159*, 31 January 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; W Caelli, *Submission PR 99*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007.

107 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; W Caelli, *Submission PR 99*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007.

108 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Security Intelligence Organisation, *Submission PR 180*, 9 February 2007; Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159*, 31 January 2007.

109 'Communication' is the terminology used in the *Intelligence Services Act 2001* (Cth). Sections 6 (1)(b), 6B(d) and 7(b) of the *Intelligence Services Act 2001* (Cth) provide that one of the functions of the ASIS, the DIGO and the DSD is to communicate, in accordance with the requirements of the Australian Government, intelligence about specified matters.

110 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159*, 31 January 2007.

111 Ibid; Australian Security Intelligence Organisation, *Submission PR 180*, 9 February 2007.

112 Australian Security Intelligence Organisation, *Submission PR 180*, 9 February 2007.

113 Ibid.

114 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159*, 31 January 2007.

115 Australian Security Intelligence Organisation, *Submission PR 180*, 9 February 2007.

34.66 The OPC and the intelligence and defence intelligence agencies were of the view that the privacy requirements applying to the intelligence and defence intelligence agencies were adequate, including legislative requirements, ministerial directions and secrecy provisions.[116] The foreign intelligence agencies also submitted that they have invested resources and conducted internal audits to monitor and ensure adherence to the privacy rules and other relevant legislative and administrative requirements.[117]

34.67 Furthermore, ASIO and the foreign intelligence agencies stated that they already are subject to robust accountability and oversight mechanisms, including through the IGIS and the PJCIS.[118] In addition, ASIO suggested that the current exemption that applies to it is consistent with international standards under the OECD Guidelines, the EU Directive and the APEC Privacy Framework.[119]

34.68 By contrast, the Queensland Council of Civil Liberties expressed concern that there is a danger that intelligence agencies may regard themselves as exempt from control and supervision, and suggested that other mechanisms should be implemented to ensure that these agencies are accountable.[120]

34.69 The OPC noted that the IGIS has been developed as a specialist oversight body for intelligence and defence intelligence agencies due to the different nature of the work of these agencies. The OPC submitted that 'it may be difficult for the Privacy Commissioner to investigate or audit the activities of [these] agencies without the appropriate powers, infrastructure or security clearances'.[121]

34.70 The Centre for Law and Genetics submitted that the exemption of these agencies is reasonable, but only should apply when an officer of an intelligence or defence intelligence agency is acting in the public interest. The exemption should not apply when such an officer is seeking personal information for private purposes. It also suggested that, as a matter of good practice, any access to personal information by these agencies should be recorded to enable access to be tracked and later audited.[122]

34.71 A few stakeholders suggested that, although there is a legitimate public interest in exempting the intelligence and defence intelligence agencies from compliance with

---

116 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007; Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159,* 31 January 2007.

117 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159,* 31 January 2007.

118 Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007; Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159,* 31 January 2007.

119 Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007.

120 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

121 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

122 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

the *Privacy Act*, these agencies should not be exempt completely from the Act.[123] These stakeholders suggested that the exemption may not be justified in respect of administrative information,[124] or staff and contractors' records of the intelligence and defence intelligence agencies.[125]

34.72 Only the foreign intelligence agencies commented on whether any other intelligence and defence intelligence agencies should be exempt from the operation of the *Privacy Act*. Only one possibility was mentioned—the Defence Security Authority, which is a member of the Intelligence and Security Group within the Department of Defence. The common view, however, was that the Defence Security Authority should not be exempt from the operation of the Act.[126]

34.73 In DP 72, the ALRC expressed the preliminary view that there is a need to balance privacy interests with the public interest in maintaining national security and defence. The ALRC observed that the ability to collect and assess intelligence information covertly is central to the functions of the intelligence and defence intelligence agencies. Given the inherently covert nature of much of the work of these agencies, many of the requirements under the privacy principles would be incompatible with their functions—especially those requirements in the proposed Unified Privacy Principles (UPPs) relating to collection, use and disclosure, and notification.

34.74 The ALRC noted that each of the intelligence and defence intelligence agencies is subject to privacy rules or guidelines, and that the IGIS generally has been satisfied with the implementation of, and compliance with, those rules and guidelines by such agencies. The ALRC stated that there is room, however, for extending the ambit of the privacy rules and guidelines, and improving the relevant legislative arrangements for, and the accessibility of, the rules and guidelines. The ALRC therefore made a number of proposals to improve the consistency and accessibility of the rules and guidelines and to strengthen the relevant legislative arrangements. These proposals included:

---

123 Commonwealth Ombudsman, *Submission PR 202*, 21 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; K Pospisek, *Submission PR 104*, 15 January 2007.

124 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

125 Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

126 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 159*, 31 January 2007. The Defence Security Authority is responsible for the coordination of security across the Department of Defence, including the development of security policy, security training and awareness across the Department of Defence and the Australian Defence Force; security performance assessment programs; serious and complex security investigations; and security vetting of personnel: Australian Government Department of Defence, *Annual Report 2004–05* (2005), 244.

- amendment of the privacy rules and guidelines to ensure consistency in relation to incidents involving the incorrect use and disclosure of personal information, and the accuracy, storage and security of personal information;[127]

- a legislative requirement that ministers responsible for the ONA and the DIO make written rules regulating the agencies' communication and retention of intelligence information concerning Australian persons;[128]

- amendment of the relevant enabling legislation to ensure that the ministers responsible for the intelligence and defence intelligence agencies consult with the OPC before making privacy rules or guidelines;[129] and

- a requirement that the privacy rules and guidelines be made available electronically to the public, for example, on the website of those agencies.[130]

Submissions and consultations

34.75 Several stakeholders supported the approach proposed by the ALRC concerning the intelligence and defence intelligence agencies.[131] For example, National Legal Aid supported the proposals on the basis that:

> Australian citizens and residents facing the exercise of extraordinary powers under anti-terrorist legislation need to have at least some basic assurance of the integrity of the information giving rise to investigation and charges.[132]

34.76 One individual suggested that the guidelines provide insufficient protection of the personal information handled by intelligence and defence intelligence agencies.[133] The Cyberspace Law and Policy Centre argued that these agencies should not be exempt completely from the *Privacy Act* and that 'the extent of any justifiable exemptions to or modifications of specific IPPs should be stated in the Schedule to the Act'. It suggested there was no justification for the exemption of intelligence and defence intelligence agencies in respect of administrative and employment information. It also suggested that some of the privacy principles should apply to all personal information handled by the intelligence and defence intelligence agencies, including information collected operationally. The Cyberspace Law and Policy Centre suggested the following principles should apply: data security; data quality; and the use and

---

127 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 31–1.
128 Ibid, Proposals 31–2(a), 31–3(a).
129 Ibid, Proposals 31–2(b), 31–3(b), 31–4.
130 Ibid, Proposal 31–5.
131 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; 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.
132 National Legal Aid, *Submission PR 521*, 21 December 2007.
133 Confidential, *Submission PR 332*, 19 October 2007.

disclosure principle, provided that there are specific exceptions for use and disclosure that is required by law or for law enforcement purposes.[134]

Consistent privacy rules and guidelines

34.77 In submissions there was support[135] for the proposal that the privacy rules and guidelines applicable to the intelligence and defence intelligence agencies be amended to include consistent rules and guidelines relating to incidents involving the incorrect use and disclosure of personal information, and the accuracy, storage and security of personal information.[136]

34.78 Privacy NSW agreed that the privacy rules and guidelines should be consistent, given the covert nature of activities of the intelligence and defence intelligence agencies, and stressed that there is a 'need for a transparent framework issued by the OPC governing law enforcement and intelligence agencies'.[137]

34.79 The Law Council of Australia submitted that the argument that the intelligence and defence intelligence agencies should be exempt, because they already are subject to specific privacy rules and guidelines, would be sustainable only if the relevant rules and guidelines address the full spectrum of issues dealt with under the *Privacy Act*. The Law Council argued that, to the extent that those rules and guidelines 'are currently focused on [the] collection, communication and retention of information … they cannot provide an adequate substitute for the *Privacy Act*'.[138]

34.80 On the other hand, the foreign intelligence agencies submitted that the privacy rules and guidelines already address the incorrect use and disclosure of personal information, as well as the storage and security of information. In relation to the incorrect use and disclosure of personal information, they submitted that they already are required to advise the IGIS of such incidents, and to either consult with the IGIS to determine the appropriate remedial action, or advise the IGIS of the incident and the measures taken to protection the privacy of the Australian person. In addition, the agencies stated that, in practice, intelligence is 'used' when it is communicated, and that any use of personal information that did not fall within their statutory functions

---

134 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

135 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; 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; P Youngman, *Submission PR 394*, 7 December 2007.

136 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 31–1.

137 Privacy NSW, *Submission PR 468*, 14 December 2007.

138 Law Council of Australia, *Submission PR 527*, 21 December 2007.

and powers would be 'incorrect' and subject to investigation by the IGIS pursuant to s 8 of the IGIS Act.[139]

34.81 As regards the storage and security of personal information, the foreign intelligence agencies argued that the requirements under the privacy rules and guidelines, together with the *Protective Security Manual* and penalties under the *Crimes Act 1914* (Cth), already exceed the requirements under the *Privacy Act*. They noted that the privacy rules and guidelines currently require that intelligence information concerning Australian persons be retained by the intelligence and defence intelligence agencies in a manner applicable to the retention of information having a security classification of not less than 'secret'. The foreign intelligence agencies noted that the *Protective Security Manual* already includes 'requirements for storing material; procedures for registering, transferring and reproducing classified material; and restrictions on who can handle such information'. In addition, it was observed that any deliberate disclosure of information classified as 'secret' would be subject to penalties under the *Crimes Act*.[140]

34.82 The foreign intelligence agencies also submitted that the intent of the proposal that there should be consistent privacy rules and guidelines concerning the accuracy of personal information was unclear. They argued that the proposal appeared to be at odds with their functions. Their submission was that, since intelligence is focused on the intentions, activities and capabilities of individuals or organisations, it is rarely simple factual information or information that is readily verifiable.

> Rather, it is the credibility of information that matters. Collection agencies are obliged to report intelligence information they have collected accurately, whether or not it is true. This allows assessment agencies to test the credibility of that intelligence against all other available information and develop assessments for government accordingly. In these senses, accuracy is at the very heart of the intelligence processes. However, the processes are conceptually quite different and attempting an overlay applicable to other areas of public administration would not be appropriate.[141]

Written privacy rules for DIO and ONA

34.83 A number of stakeholders[142] supported the proposals that would require ministers responsible for the ONA and the DIO to make written rules regulating the agencies' communication and retention of intelligence information concerning

---

139 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466*, 13 December 2007.

140 Ibid.

141 Ibid.

142 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007 (supported the responsible minister for ONA being required to make such written rules); Privacy NSW, *Submission PR 468*, 14 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

Australian persons.[143] The Office of the Victorian Privacy Commissioner (OVPC) was concerned that the proposals only related to 'the privacy of Australian persons', and considered that there is 'no policy justification for limiting the privacy protections to Australian citizens or permanent residents'.[144]

34.84 The foreign intelligence agencies did not support the proposals. They suggested that, since a core area of the activities of foreign intelligence collection agencies—ASIS, the DSD and the DIGO—is to gather intelligence from various sources, it is possible that these agencies may collect intelligence about Australian individuals and therefore a legislative requirement to adhere to privacy rules is appropriate. It was observed that, by contrast, foreign intelligence assessment agencies—the ONA and the DIO—generate assessments using information from a number of sources, including intelligence provided by collection agencies that has been collected in accordance with the applicable privacy rules. They argued, therefore, that subjecting the assessment agencies to administrative privacy guidelines (rather than privacy rules mandated by legislation) is appropriate given the lower level of risk to privacy posed by the activities of such agencies.[145]

34.85 The foreign intelligence agencies also submitted that, due to their international focus, 'foreign intelligence reporting on an Australian is relatively rare and instances where an Australian might be mentioned are few'. In addition, the agencies submitted that the privacy guidelines applicable to the ONA and the DIO are very similar to the privacy rules applicable to the ASIS, the DIGO and the DSD, and that the ONA and the DIO also are subject to similar reporting and monitoring requirements as those imposed on the foreign intelligence collection agencies.[146]

Consultation with the OPC

34.86 A number of stakeholders supported the proposals that ministers responsible for the intelligence and defence intelligence agencies be required to consult with the OPC before making rules to protect the privacy of Australian persons.[147] The OPC supported

---

143 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 31–2(a), 31–3(a).

144 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

145 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466*, 13 December 2007.

146 Ibid.

147 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 31–2(b), 31–3(b), 31–4. The following submissions supported the proposals relating to ASIS, DIGO, DSD, DIO and ONA: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; P Youngman, *Submission PR 394*, 7 December 2007. The following submissions supported the proposal as it relates to ASIO: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008;

the proposals, but noted that such consultation should be held with the Privacy Commissioner rather than his or her office. It also noted that the Privacy Commissioner has been consulted on ASIO's privacy guidelines on a previous occasion.[148] The Public Interest Advocacy Centre (PIAC) supported the proposal, but suggested that there needs to be further clarification as to whether the relevant ministers also should consult with the IGIS and the Attorney-General.[149]

34.87 The Law Council of Australia supported the proposal as it relates to ASIO, but submitted that s 8A(6) of the ASIO Act also should explicitly require the minister responsible for ASIO to consult with the IGIS in the drafting stage—even though it was understood that this does occur in practice. The Law Council also noted that when the new ASIO guidelines were issued in October 2007, the IGIS was reportedly dissatisfied with the guidelines and troubled by the absence of substantial requirements concerning retention and destruction of intelligence information. It was submitted that:

> These reported comments demonstrate that an obligation to consult with IGIS and the OPC will only ever provide a limited safeguard and should not be regarded as a substitute for enforceable duties and standards.[150]

34.88 On the other hand, the foreign intelligence agencies did not support the proposals, on the grounds that 'the existing framework for oversight of agencies' privacy provisions by the IGIS and the Attorney-General provides for strong oversight and accountability', and that the proposal appeared to risk duplication with the role of the IGIS. In addition, they argued that the current privacy rules and guidelines were developed in consultation with the Attorney-General, the relevant agency head and the IGIS.[151]

Public availability of privacy rules and guidelines

34.89 A number of stakeholders,[152] including the foreign intelligence agencies and the IGIS,[153] agreed that the privacy rules and guidelines applicable to the intelligence and

---

Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Law Council of Australia, *Submission PR 527*, 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.

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

149 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

150 Law Council of Australia, *Submission PR 527*, 21 December 2007.

151 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466*, 13 December 2007.

152 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

153 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466*, 13 December 2007; Inspector-General of Intelligence and Security, *Submission PR 432*, 10 December 2007.

defence intelligence agencies should be made available to the public electronically.[154] In his submission, the IGIS stated that making the privacy rules and guidelines readily available to the public is appropriate and involves 'no significant security considerations'. In addition, the IGIS considered that 'there is benefit in making available information about the ways in which the agencies are held to account'.[155]

34.90 The Law Council of Australia stated that 'the public dissemination of information about the powers and obligations of intelligence agencies is a pre-requisite to accountability'. It submitted further that the privacy rules and guidelines should be highlighted clearly on an agency's website so that members of the public would not have to know that the specific rules and guidelines exist or their precise titles in order to be able to locate them.[156]

34.91 The OPC supported the proposal, but suggested that 'reasonable steps should be taken to ensure that the privacy rules and guidelines [are] made available in other accessible forms as requested by members of the public', which would enhance community confidence in the agencies' handling of personal information.[157] Similarly, the OVPC submitted that 'these rules and guidelines should be made available in a variety of formats, both electronic and hard copy and preferably, in a range of community languages'.[158]

34.92 While supportive of the proposal, the Australian Privacy Foundation and PIAC suggested that the relevant legislative provisions requiring the making of privacy rules also should be made available to the public electronically.[159] The ALRC notes that the relevant legislative provisions are readily accessible on the 'ComLaw' website maintained by the AGD.[160] In the ALRC's view, the current level of accessibility of the relevant provisions is adequate.

34.93 The IGIS, while not commenting in detail on the proposals concerning the intelligence and defence intelligence agencies, submitted that the current accountability arrangements clearly are significant and effective. On this basis, the IGIS stated that 'it is understandable that intelligence and defence intelligence agencies might question why there is any need for changes to existing structures'.[161]

---

154 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 31–5.
155 Inspector-General of Intelligence and Security, *Submission PR 432*, 10 December 2007.
156 Law Council of Australia, *Submission PR 527*, 21 December 2007.
157 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
158 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
159 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
160 See <www.comlaw.gov.au/>.
161 Inspector-General of Intelligence and Security, *Submission PR 432*, 10 December 2007.

ALRC's view

34.94 The current exemptions that apply to the intelligence and defence intelligence agencies under the *Privacy Act* should remain. Stakeholders that commented on these exemptions acknowledged the need to balance the interests of individual privacy with the interests of national security and defence. The need for such a balance is consistent with international standards, which provide for exceptions or exemptions to privacy principles for the purposes of national security and defence.

34.95 The central function of intelligence and defence intelligence agencies is the covert collection and assessment of intelligence information—that is, information 'obtained without the authority of the government or group that "owns" the information'.[162] Given the inherently covert nature of much of the work of these agencies, many of the requirements under the model UPPs would be incompatible with their functions—especially those relating to the collection, use and disclosure of personal information, and notification to the individual concerned about the information collected.

34.96 Although the intelligence agencies—ASIO, ASIS and the ONA—are exempt completely from the operation of the *Privacy Act*, and the defence intelligence agencies—the DIO, the DIGO and the DSD—are exempt partially from the operation of the Act, each of these agencies has privacy rules or guidelines in place. In addition, there is a system of accountability that provides a high degree of oversight of the intelligence and defence intelligence agencies, including oversight of compliance with the privacy rules and guidelines by the IGIS. The ALRC is generally satisfied with the degree and quality of oversight of the intelligence and defence intelligence agencies.

34.97 While the IGIS has reported his overall satisfaction with the implementation of, and compliance with, the privacy rules and guidelines by the intelligence and defence intelligence agencies, the ALRC considers that there is room for extending the ambit of the privacy rules and guidelines, and improving the relevant legislative arrangements and the accessibility of the rules and guidelines.

34.98 First, the privacy rules and guidelines applicable to intelligence and defence intelligence agencies currently only cover Australian persons. There is merit in the OVPC's submission that the privacy protections provided by these rules and guidelines should not be limited to Australian persons. The ALRC is of the view, however, that the coverage of the privacy rules and guidelines should be extended to the handling of personal information about non-Australian individuals only to the extent that this is covered by the *Privacy Act*. This is because the privacy rules and guidelines applicable to intelligence and defence intelligence agencies should not have a more extensive extra-territorial operation than the *Privacy Act*.

---

162 Australian Government Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 3.

34.99 While the *Privacy Act* generally covers the handling of personal information about an individual—which is defined as a natural person under s 6(1) and therefore is not limited to Australian individuals—it extends to overseas acts and practices of an organisation only where:

> the act or practice relates to personal information about an Australian citizen or a person whose continued presence in Australia is not subject to a limitation as to time imposed by law …[163]

34.100 The ALRC recommends, therefore, that the privacy rules and guidelines applicable to the intelligence and defence intelligence agencies be extended to cover the *domestic* acts and practices of these agencies relating to personal information about non-Australian individuals. These privacy rules and guidelines, however, should not cover the *overseas* acts and practices of an intelligence agency or a defence intelligence agency unless those acts and practices relate to personal information about an Australian citizen or a person whose continued presence in Australia is not subject to a limitation imposed by law as to time.

34.101 Secondly, the governing legislation, and privacy rules and guidelines that apply to the intelligence and defence intelligence agencies only cover collection, communication and retention of intelligence information. The *Protective Security Manual* does contain minimum standards concerning the use, access, copying, storage, security and disposal of classified information. It only applies to security classified information, however, and does not deal with other matters under the UPPs. The privacy rules and guidelines should be updated, therefore, to include rules dealing with the incorrect use and disclosure by intelligence and defence intelligence agencies of all personal information, the accuracy of records, and the storage and security of personal information.

34.102 The ALRC notes the submission by the foreign intelligence agencies that the privacy rules and guidelines applicable to them already require that they notify the IGIS of incidents involving the incorrect use and disclosure of personal information. The Attorney-General's Guidelines, however, do not contain a similar requirement. The ALRC is of the view that the Attorney-General's Guidelines should be amended in line with the other privacy rules and guidelines in this regard.

34.103 In relation to the accuracy of records, the ALRC agrees with the submission by the foreign intelligence agencies that some intelligence may not be verifiable information. This issue should be covered in the drafting of the privacy rules and guidelines. It is clear that there may be circumstances where it would be unreasonable to require an intelligence agency or a defence intelligence agency to verify the accuracy of certain personal information, for example, because it would alert the

---

163 *Privacy Act 1988* (Cth) s 5B(1)(a).

intelligence target to the agency's covert investigation. This calls for the use of qualitative or evaluative terms, such as 'fair and reasonable', in the drafting of the accuracy requirement, rather than the omission of accuracy requirements. Such an approach allows the same rules to apply flexibly to the individual intelligence and defence intelligence agencies within their different operational contexts. Accordingly, the ALRC recommends that the privacy rules and guidelines applicable to the intelligence and defence intelligence agencies be amended to include consistent rules and guidelines relating to the accuracy of personal information.

34.104 As regards storage and security of personal information, the ALRC notes that the need for rules concerning the retention and destruction of personal information was highlighted by the IGIS's dissatisfaction with the 2007 Attorney-General's Guidelines. The IGIS reportedly was unable to endorse the new guidelines in their entirety because of concerns about the lack of substantive requirements as to when ASIO should retain or destroy data.[164] The ALRC therefore recommends that the privacy rules and guidelines applicable to the intelligence and defence intelligence agencies include consistent rules and guidelines relating to the storage and security of personal information.

34.105 Thirdly, under the ASIO Act and the *Intelligence Services Act*, the ministers responsible for ASIO, ASIS, the DSD and the DIGO are required to make written rules regulating the communication and retention of intelligence information concerning Australian persons. Although the ONA and the DIO have implemented privacy guidelines administratively, their responsible ministers are not subject to the same legislative requirement to make written rules or issue ministerial guidelines as other intelligence and defence intelligence agencies. The ALRC considers this anomaly should be corrected by an amendment to the *Intelligence Services Act* and the *Office of National Assessments Act* that requires the ministers responsible for the ONA and the DIO to make written rules regulating the handling of intelligence information about individuals by the agencies.

34.106 The ALRC notes the submission by the foreign intelligence agencies that the ONA and the DIO should be subject only to privacy guidelines (rather than privacy rules mandated by legislation) because of the lower level risk they pose to privacy compared to other foreign intelligence agencies. While this may be the case, the ALRC does not agree that intelligence and defence intelligence agencies should be treated differently based on the different level of risk they pose to privacy. The ALRC's approach in this Report is that, subject to limited exceptions, privacy regulation should apply universally, regardless of the degree of risk an agency or organisation poses to privacy. By analogy, the different levels of risk posed by individual intelligence and defence intelligence agencies do not provide sufficient justification for them to be subject to different requirements concerning privacy.

---

164 N O'Brien, 'Changes Permit ASIO to Keep Files', *The Australian* (online), 13 October 2007, <www.theaustralian.news.com.au>.

34.107 Furthermore, not all of the ministers responsible for the intelligence and defence intelligence agencies are required to undertake a consultation process before making privacy rules or guidelines. The ministers responsible for ASIS, the DIGO and the DSD are required to consult with the relevant agency head, the IGIS and the Attorney-General when drafting privacy rules; however, there is no equivalent provision that applies to the other intelligence and defence intelligence agencies.[165] In addition, none of the ministers are required to consult with the Privacy Commissioner when drafting such rules. In the ALRC's view, all ministers with responsibility for the intelligence and defence intelligence agencies should consult with the appropriate agencies before making privacy rules. The appropriate agencies would include the relevant agency heads and the IGIS, who have responsibility for, or oversight of, the activities of the relevant agencies, and the Privacy Commissioner and the minister responsible for administering the *Privacy Act*, who oversee privacy regulation in Australia.

34.108 Finally, the ALRC recommends that the privacy rules and guidelines should be made more accessible to the public. In DP 72, the ALRC noted that, although all of the privacy rules and guidelines applicable to the intelligence and defence intelligence agencies were available electronically on the IGIS's website, and some of them are available on the relevant agency's website, those applicable to the ONA and the DIO were not available on the agencies' websites. Since the publication of DP 72, the ONA has posted its privacy guidelines on its website. The DIO is now the only relevant agency that has not made its privacy guidelines available electronically on its website. All privacy rules and guidelines should be published on the relevant agency's website and should be made available, on request, in other accessible forms.

34.109 A few stakeholders suggested that the intelligence and defence intelligence agencies should be subject to exceptions to specific privacy principles, rather than exempt from the operation of the *Privacy Act*. The ALRC disagrees with this approach. All the intelligence and defence intelligence agencies already are subject to privacy rules or guidelines. The ALRC also is recommending that the ambit of these rules and guidelines be extended further to enhance privacy protection. In addition, the internal processes and methods of the intelligence and defence intelligence agencies are subject to a number of oversight and accountability mechanisms, including by the IGIS, the PJCIS and others. In particular, the IGIS has reported that he conducted regular inspections of the intelligence and defence intelligence agencies and actively monitored their adherence to privacy rules and guidelines. Finally, it should be noted that the OPC would have difficulties investigating or auditing the activities of the intelligence and defence intelligence agencies because it lacks the appropriate powers, infrastructure and security clearances to do so. For these reasons, it is not necessary to

165 *Intelligence Services Act 2001* (Cth) s 15(3).

alter the scope of the exemption that applies to the intelligence and defence intelligence agencies under the *Privacy Act*.

Recommendation 34–1 (a) The privacy rules and guidelines that relate to the handling of intelligence information concerning Australian persons by the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate and the Office of National Assessments, should be amended to include consistent rules and guidelines relating to:

(i) the handling of personal information about non-Australian individuals, to the extent that this is covered by the *Privacy Act*;

(ii) incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of incidents and measures taken to protect the privacy of the individual);

(iii) the accuracy of personal information; and

(iv) the storage and security of personal information.

(b) The privacy rules and guidelines should be made available without charge to an individual: electronically on the websites of those agencies; and on request, in hard copy or, where reasonable, in an alternative form accessible to individuals with special needs.

Recommendation 34–2 Section 15 of the *Intelligence Services Act 2001* (Cth) should be amended to provide that the ministers responsible for the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate and the Defence Intelligence Organisation:

(a) are required to make written rules regulating the handling of intelligence information concerning individuals by the relevant agency, except where:

(i) the agency is engaged in activity outside Australia and the external territories; and

(ii) that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law; and

(b) should consult with the relevant agency head, the Privacy Commissioner, the Inspector-General of Intelligence and Security and the minister responsible for administering the *Privacy Act* before making privacy rules about the handling of intelligence information.

Recommendation 34–3 The *Office of National Assessments Act 1977* (Cth) should be amended to provide that the minister responsible for the Office of National Assessments (ONA):

(a) is required to make written rules regulating the handling of intelligence information about individuals by the ONA, except where:

(i) the ONA is engaged in activity outside Australia and the external territories; and

(ii) that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law; and

(b) should consult with the Director-General of the ONA, the Privacy Commissioner, the Inspector-General of Intelligence and Security and the minister responsible for administering the *Privacy Act* before making privacy rules about the handling of intelligence information.

Recommendation 34–4 Section 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth) should be amended to provide that the:

(a) guidelines issued by the minister responsible for the Australian Security Intelligence Organisation (ASIO) must include guidelines regulating the handling of intelligence information about individuals by ASIO, except where ASIO:

(i) is engaged in activity outside Australia and the external territories; and

(ii) that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law; and

(b) minister responsible for ASIO should consult with the Director-General of Security, the Privacy Commissioner, the Inspector-General of Intelligence and Security and the minister responsible for administering the *Privacy Act* before making privacy guidelines about the handling of intelligence information.

Inspector-General of Intelligence and Security

Background

34.110 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office within the Prime Minister's portfolio. The IGIS was set up under the IGIS Act to ensure that certain intelligence and security agencies conduct their activities within the law, behave with propriety, comply with ministerial guidelines and directions, and have regard to human rights. He or she monitors the activities of intelligence and defence intelligence agencies regularly, conducts inquiries, investigates complaints about these agencies, makes recommendations to the government and provides annual reports to the Australian Parliament.[166]

34.111 Under existing law, the IGIS, as an agency listed in Schedule 2, Part I, Division 1 of the FOI Act, is exempt from compliance with the IPPs.[167] He or she is subject to other provisions of the Act, however, such as the tax file number provisions. In addition, as an exempt agency under the FOI Act, the IGIS is not required under that Act to provide access to information. No policy justification has been given for the IGIS's exemption from the operation of the *Privacy Act*. Therefore, the exemption appears to derive from the fact that the IGIS is listed under Schedule 2, Part I of the FOI Act.

34.112 In the 1994 inquiry into the FOI Act, the ALRC and ARC commented that decisions to exempt particular agencies from the FOI Act have tended to be selective.[168] The ALRC and ARC were of the view, however, that the exemption of the IGIS from the operation of the FOI Act was warranted and recommended that the IGIS and other intelligence agencies should remain in Part I of the Act as exempt agencies.[169]

34.113 Currently, there are no privacy rules or guidelines that apply to the IGIS. The IGIS is, however, required to comply with the *Protective Security Manual* and is

---

166 *Inspector-General of Intelligence and Security Act 1986* (Cth) pt II; Inspector-General of Intelligence and Security, *Frequently Asked Questions* <www.igis.gov.au/faq's.cfm> at 7 April 2008.

167 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2).

168 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

169 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 74.

subject to secrecy provisions. Part C of the *Protective Security Manual* sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information. The privacy protections under the *Protective Security Manual*, however, are restricted to security classified information and do not deal with other matters under the IPPs, such as the accuracy of personal information. In relation to secrecy, under the IGIS Act, the IGIS or a staff member is prohibited from making a record, or divulging or communicating any information acquired by reason of the person holding or acting in that office.[170] The records of the IGIS also are subject to the *Archives Act 1983* (Cth), which deals with the custody, destruction and disposal of Commonwealth records, including the records of the IGIS.[171]

34.114 The IGIS is directly accountable to the Prime Minister and must provide the Prime Minister annually with a report on the IGIS's activities. The Prime Minister may make deletions from the IGIS's annual report before tabling it in Parliament, if he or she considers that the deletion is necessary 'to avoid prejudice to security, the defence of Australia, Australian's relations with other countries or the privacy of individuals'. A full copy of the report is provided to the Leader of the Opposition, who must treat as secret any part of the report that is not tabled in Parliament.[172]

34.115 In Canada and New Zealand, bodies overseeing the work of security and intelligence agencies are subject to privacy legislation, but may refuse to disclose personal information under certain circumstances. In Canada, the Office of the Inspector General of the Canadian Security Intelligence Service and the Security Intelligence Review Committee are subject to federal privacy legislation.[173] They may refuse to disclose any personal information requested, however, if the information was obtained or prepared by any government institution that is a specified investigative body in the course of lawful investigations relating to activities suspected of constituting threats to the security of Canada.[174]

34.116 Similarly, in New Zealand, the Inspector-General of Intelligence and Security and the Intelligence and Security Committee are covered by the *Privacy Act 1993* (NZ). They may refuse to disclose any information, however, if the disclosure would be likely to prejudice: the security or defence of New Zealand; the international

---

170 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34.

171 Section 6 of the *Archives Act 1983* (Cth) empowers the National Archives of Australia to acquire or authorise the disposal or destruction of Commonwealth records, except specified exempt records. Exempt records include, for example, information or matter the disclosure of which could reasonably be expected to cause damage to the security, defence or international relations of the Commonwealth; and information communicated in confidence by or on behalf of a foreign government, an authority of a foreign government or an international organisation, the disclosure of which under the *Archives Act* would constitute a breach of that confidence: *Archives Act 1983* (Cth) s 33(1).

172 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 35.

173 *Privacy Act* RS 1985, c P-21 (Canada) s 3 (definition of 'government institution').

174 Ibid s 22.

relations of the Government of New Zealand; or the entrusting of information to the Government of New Zealand on a confidential basis by foreign governments, their agencies or any international organisation.[175]

34.117 In contrast, in the United Kingdom, personal data are exempt from any of the data protection principles and other provisions of the *Data Protection Act 1998* (UK) if the exemption from that provision is required for the purpose of safeguarding national security.[176]

34.118 In DP 72, the ALRC considered whether the exemption that applies to the IGIS under the *Privacy Act* should be retained. The ALRC noted that few stakeholders commented specifically on the exemption that applies to the IGIS. Several stakeholders suggested, however, that the exemption of any Australian Government agencies, including those specified in Schedule 2, Part I, Division 1 of the FOI Act, should be justified and limited to the extent possible.[177] It also was submitted that any difficulties that compliance with privacy principles might cause for such agencies should be dealt with by means of selective exceptions to particular principles.[178]

34.119 The ALRC observed that much of the personal information handled by the IGIS would have originated with, or have been received from, an intelligence agency or a defence intelligence agency, and therefore would be excluded from the operation of the *Privacy Act*. The ALRC noted, however, that other records held by the IGIS also may contain security sensitive information. Accordingly, the ALRC expressed the preliminary view that some exemption from the *Privacy Act* should continue to apply to the IGIS, but that there is no policy justification for the exemption to extend to the IGIS's administrative records. The ALRC therefore proposed that the *Privacy Act* be amended to apply to the IGIS in respect of the administrative operations of his or her office.[179] In addition, the ALRC proposed that the IGIS, in consultation with the OPC, develop and publish information-handling guidelines to ensure that the personal information handled by the IGIS is protected adequately.[180]

Submissions and consultations

34.120 There was support, including from the IGIS, for the proposal that the *Privacy Act* be amended to apply to the IGIS in respect of the administrative operations of that

---

175 *Privacy Act 1993* (NZ) s 27.

176 *Data Protection Act 1998* (UK) s 28.

177 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

178 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

179 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 31–6.

180 Ibid, Proposal 31–7.

office.[181] The IGIS stated that he considered the proposal to be 'both reasonable and practically achievable', and noted that it would be

> most unlikely that subjecting … administrative records [of the office of the IGIS] to the requirements of the *Privacy Act* would reduce the effectiveness of the agency or compromise national security.[182]

34.121 The OVPC supported the proposal, on the basis that the exemption provision should be limited to specific acts and practices rather than the entire entity.[183]

34.122 The OPC did not have any specific comment on the substance of the ALRC's proposal, but suggested that 'entities with similar functions [should] be treated consistently under the *Privacy Act's* exemption provisions'. The OPC also stated that the proposal is consistent with the OPC's general position that exemptions from the operation of the *Privacy Act* should be minimised, and justified on the basis of clear and compelling public interest.[184]

34.123 A number of stakeholders supported the proposal that the IGIS, in consultation with the OPC, develop and publish information-handling guidelines.[185] For example, the OPC stated that all entities, regardless of whether they are covered by the *Privacy Act*, should implement a set of information-handling standards. It suggested that information-handling standards for the IGIS could be adapted from the privacy principles, while taking into account the requirements of national security. The OPC also noted that it would be appropriate for the minister responsible for the IGIS to consult with the Privacy Commissioner specifically, rather than with the OPC.[186]

34.124 The OVPC submitted that guidelines may be an appropriate way to provide some protection for personal information gathered by the IGIS from state databases. The OVPC also argued that, while there may be good reasons for exemptions,

---

181 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Inspector-General of Intelligence and Security, *Submission PR 432*, 10 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

182 Inspector-General of Intelligence and Security, *Submission PR 432*, 10 December 2007.

183 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

185 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

guidelines promote transparency by communicating the reasons for the collection of personal information.[187]

34.125 The IGIS, however, did not support the proposal. He suggested that the proposed information-handling guidelines would not increase the level of protection provided by the current 'robust and reasonable protective framework' for personal information handled by the IGIS. The IGIS submitted that, while there are currently no information-handling guidelines that are specific to the IGIS, his office

> handles personal information in accordance with protocols and procedures that are entirely consistent with the policy objectives of the *Privacy Act* and necessarily closely aligned with those of the [Australian intelligence community].[188]

34.126 The IGIS advised that his office handles three broad categories of personal information: (a) information relating to employees; (b) information distributed to the office of the IGIS in the intelligence product of the intelligence and defence intelligence agencies or otherwise accessed in the course of the work of that office; and (c) information received from members of the Australian public. In relation to personal information of employees, the IGIS stated that the adoption of the proposal that the IGIS be covered by the *Privacy Act* in respect of the administrative operations of his or her office would make it unnecessary to subject the IGIS to information-handling standards.[189]

34.127 The IGIS submitted that personal information contained in the intelligence and defence intelligence agencies' intelligence product is rightly exempt from the *Privacy Act*. The IGIS considered that subjecting such personal information to information-handling guidelines would be inconsistent with the policy objective underlying s 7(1)(f) of the *Privacy Act*, which excludes from the coverage of the Act personal information that has originated, or been received from, an intelligence agency or a defence intelligence agency.[190]

34.128 As regards personal information received by the IGIS from members of the public, the IGIS submitted that this category of personal information has a connection with records that originated with, or was received from, an intelligence agency or a defence intelligence agency. The information usually relates to complaints made by members of the public about such an agency. The IGIS stated that the IGIS's protocols and procedures for the management of that information reflect the existing framework set out in the IGIS Act, the *Archives Act* and the *Protective Security Manual*—and, in particular, the secrecy provision under s 34 of the IGIS Act, which establishes a robust legislative regime protecting information handled by the IGIS. The IGIS stated that he was 'particularly conscious of the impact an allegation or finding of misuse of

---

187 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
188 Inspector-General of Intelligence and Security, *Submission PR 432*, 10 December 2007.
189 Ibid.
190 Ibid.

information, including unauthorised disclosure, would have on [the] office'. He submitted that the effectiveness of the existing protocols and procedures is demonstrated by the fact that 'in the 20 years since [the] office was established there has never been a credible or substantiated allegation of this kind made'.[191]

ALRC's view

34.129 The IGIS performs an important oversight role in ensuring that intelligence and defence intelligence agencies act legally, with propriety, in compliance with ministerial directions and with regard to human rights. In performing this role, the IGIS handles records that have originated with, or have been received from, these agencies. Consequently, much of the personal information handled by the IGIS would have originated with, or have been received from, the intelligence and defence intelligence agencies. Although these records are excluded from the operation of the *Privacy Act*, other records held by the IGIS also may contain security sensitive information—for example, such information may be contained in the IGIS's internal working documents that relate to the work of the intelligence and defence intelligence agencies. Accordingly, the ALRC is of the view that some exemption from the *Privacy Act* should continue to apply to the IGIS.

34.130 There is, however, no policy justification for the exemption to extend to the IGIS's administrative records. Unlike the intelligence and defence intelligence agencies, the IGIS is not bound by ministerial privacy rules or guidelines and its operations are subject only to oversight by the Prime Minister. The ALRC recommends, therefore, that the IGIS be brought under the *Privacy Act* in respect of his or her office's administrative operations, such as the handling of employee records. The ALRC notes that this was supported by the IGIS, who stated that coverage of IGIS's administrative operations under the *Privacy Act* would be unlikely to affect the effectiveness of his office or compromise national security. In light of the above, the ALRC agrees with the IGIS that it would be unnecessary to subject the IGIS's administrative records to additional information-handling guidelines.

34.131 In Chapter 33, the ALRC expresses the view that, where an entity is exempt, either completely or partially, from the operation of the *Privacy Act*, appropriate information-handling guidelines should be in place to ensure that the handling of personal information not covered by the Act would be protected adequately. As noted above, the handling of records that have originated with, or have been received from, an intelligence agency or a defence intelligence agency by the IGIS is not subject to any specific privacy rules or guidelines. While the existing framework set out in the IGIS Act, the *Archives Act* and the *Protective Security Manual* addresses some privacy issues, it does not deal with other matters under the UPPs, including openness, data quality and cross-border data flows. As a matter of best practice, therefore, the IGIS

191 Ibid.

should be subject to information-handling guidelines in respect of the non-administrative operations of his or her office, to be developed and published in consultation with the OPC. The guidelines should address the full spectrum of privacy issues that are dealt with under the UPPs. The development and publication of such guidelines would promote transparency in the handling of personal information by the IGIS and help to ensure public confidence in the intelligence system.

Recommendation 34–5 The *Privacy Act* should be amended to apply to the Inspector-General of Intelligence and Security in respect of the administrative operations of that office.

Recommendation 34–6 The Inspector-General of Intelligence and Security, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines in respect of the non-administrative operations of that office.

35. Federal Courts and Tribunals

Contents

Introduction

35.1 Federal courts are currently exempt from the operation of the *Privacy Act 1988* (Cth), except in respect of matters of an administrative nature. The Australian Industrial Relations Commission, and the Industrial Registrar and Deputy Industrial Registrars, are similarly exempt. Other federal tribunals, on the other hand, are not exempt.

35.2 This chapter examines whether courts and tribunals should be exempt from the operation of the *Privacy Act* and, if so, what should be the scope of these exemptions. The ALRC concludes that the existing exemption applicable to federal courts should continue to apply, and a similar exemption, in respect of matters of an administrative nature, should apply to federal tribunals.

35.3 The chapter also discusses related matters concerning access to personal information held by courts and tribunals under the *Privacy Act*, *Freedom of Information Act 1982* (Cth) (FOI Act) and the rules of courts and tribunals.

Federal courts

Scope of the current exemption

35.4 Australian federal courts—including the High Court, the Federal Court, the Federal Magistrates Court and the Family Court[1]—fall within the definition of 'agency' in the *Privacy Act*.[2] They are covered by the Act, however, only in respect of those of their acts and practices that relate to matters 'of an administrative nature'.[3] Acts and practices of the federal courts in relation to their administrative records—including personnel records, operations and financial records, freedom of information records, complaint files and mailing lists—are covered by the *Privacy Act*.[4] Acts and practices relating to the courts' judicial records, including court lists, judgments and other documents kept by the courts relating to proceedings, are exempt.[5]

35.5 The partial exemption of federal courts from the operation of the *Privacy Act* was based on two principles: the doctrine of the separation of powers, which is embodied in the structure of the *Australian Constitution*; and the common law principle of open justice. The separation of powers requires that different institutions exercise the legislative, judicial and executive powers of the Commonwealth, and that no one institution should exercise the power or functions of the others.[6]

35.6 The principle of open justice requires that, subject to limited exceptions to protect the administration of justice, court proceedings should be open to the public.[7] Public access to court proceedings is vital to maintaining public confidence in the administration of justice.[8] Privacy issues arise, however, because personal information

---

1 The Industrial Relations Court of Australia is also a federal court. As a consequence of the *Workplace Relations and Other Legislation Amendment Act 1996* (Cth), however, the court's jurisdiction has been transferred to other courts. Despite the transfer of jurisdiction, the Industrial Relations Court continues to exist at law until the last of its judges resigns or retires from office: Federal Court of Australia, *Industrial Relations Court of Australia* <www.fedcourt.gov.au> at 30 April 2008.

2 *Privacy Act 1988* (Cth) s 6(1).

3 Ibid s 7(1)(b).

4 *I v Commonwealth Agency* [2005] PrivCmrA 6.

5 *Privacy Act 1988* (Cth) s 7(1)(a)(ii); *I v Commonwealth Agency* [2005] PrivCmrA 6. In *Re Bienstein and Family Court of Australia* [2006] AATA 385, the Administrative Appeals Tribunal (AAT) held that the organisation of court lists and the allocation of judicial officers to particular cases are not matters of an administrative nature, but 'matters affecting litigants and the public, and are intimately related to the independent and impartial administration of justice': *Re Bienstein and Family Court of Australia* [2006] AATA 385, [8].

6 *New South Wales v Commonwealth* (1915) 20 CLR 54; *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254; *Attorney-General (Cth) v The Queen* (1957) 95 CLR 529.

7 *Scott v Scott* [1913] AC 417; *Dickason v Dickason* (1913) 17 CLR 50; *Russell v Russell* (1976) 9 ALR 103.

8 *Attorney-General (UK) v Leveller Magazine Ltd* [1979] AC 440, 450. See also 'A Mutual Contempt? How the Law is Reported' (2005) 32(11) *Brief* 12, 16.

may be produced in court as a result of coercive powers and may be information that would not otherwise have entered the public arena.[9]

35.7 Certain information about matters before a court will generally be in the public arena, such as court lists and judgments, and therefore often available to non-parties. Court lists may include file numbers enabling linkage to other information held in the justice system. Court lists can be highly prejudicial to individuals because they record court appearances rather than outcomes.[10] Court judgments containing sensitive personal information may be recorded in law reports and computerised legal databases and become available to the public.[11] Other case information, such as correspondence between the courts and the parties, is generally not in the public arena but is kept on file in court registries.

Matters of an administrative nature

35.8 The *Privacy Act* does not define 'a matter of an administrative nature'. The definition of 'administration' in the *Macquarie Dictionary* suggests that 'administrative' means relating to 'the management or direction of any office or employment'.[12] In administrative law, it has been held that the expression 'decision of an administrative character' is 'incapable of precise definition' and is to be 'determined progressively in each case as particular questions arise'.[13]

35.9 Given that a comprehensive definition of 'administrative' is not possible, the courts have taken the approach of defining 'administrative' by distinguishing it from legislative and judicial actions.[14] The distinction between administrative, legislative and judicial actions also is difficult. In *Evans v Friemann*, Fox ACJ of the Federal Court stated that 'it has … proved very difficult, virtually impossible to arrive at criteria which will distinguish in all cases' the administrative, the legislative and the judicial.[15] In addition, the concepts can overlap or merge into one another,[16] and

9 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 54.

10 Ibid, 55.

11 In *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83, the AAT considered how much personal information the Tribunal may publish in its decisions. Deputy President Forgie decided that, pursuant to IPP 11, the Tribunal was required or authorised by or under law to disclose as much personal information as is necessary to meet the requirements of s 43(2B) of the *Administrative Appeals Tribunal Act 1975* (Cth), including the obligation to conduct its proceedings and decision making in public, or to disclose the intellectual processes it followed in reaching a decision.

12 *Macquarie Dictionary* (online ed, 2007).

13 *Hamblin v Duffy* (1981) 34 ALR 333, 338–339.

14 See R Creyke and J McMillan, *Control of Government Action: Text, Cases & Commentary* (2005), [2.4.25].

15 *Evans v Friemann* (1981) 35 ALR 428, 433.

16 *Hamblin v Duffy* (1981) 34 ALR 333, 338; *Evans v Friemann* (1981) 35 ALR 428, 433.

'functions may be classified as either judicial or administrative according to the way in which they are to be exercised'.[17]

35.10 One approach to distinguishing between judicial and administrative functions is to differentiate between what is 'truly ancillary to an adjudication by the court', which is incidental to the exercise of judicial power; and those that are not truly ancillary, which are administrative.[18]

35.11 A function that is 'truly ancillary to an adjudication by the court'

> must be truly subservient to adjudication. They must be undertaken pursuant to a direction by the court for the purpose of either quantifying and giving effect to an adjudication already made by the court, or of providing material upon the basis of which an adjudication by the court is to be made.[19]

35.12 In the context of freedom of information legislation, the case law suggests that documents that relate to matters of a non-administrative nature include: 'documents of the court which relate to the determination of particular matters, such as draft judgments, pleadings, documents returned under summons',[20] unrevised and unpublished transcripts of proceedings,[21] proceedings and decisions of a court held by an appellate court for the purposes of an appeal,[22] and notes relating to the provision of conciliation counselling by an officer of the court.[23] Matters of an administrative nature would include those that are unrelated to court proceedings, such as employment records, property management and contracts with suppliers; and exclude matters such as pre-trial and settlement conferences and alternative dispute resolution (ADR) work conducted by court staff. The following table shows examples of activities of the courts that are likely to be considered exempt or not exempt.

---

17 Precision Data Holdings Ltd v Wills (1991) 104 ALR 317, 325. See also J de Meyrick, 'Whatever Happened to Boilermakers? Part I' (1995) 69 Australian Law Journal 106; J de Meyrick, 'Whatever Happened to Boilermakers? Part II' (1995) 69 Australian Law Journal 189; A Hall, 'Judicial Power, the Duality of Functions and the Administrative Appeals Tribunal' (1994) 22 Federal Law Review 13, 21.

18 C Enright, *Federal Administrative Law* (2001), [22.129]; *Kotsis v Kotsis* (1970) 122 CLR 69, 92.

19 *Kotsis v Kotsis* (1970) 122 CLR 69, 92.

20 *Re Altman and the Family Court of Australia* (1992) 27 ALD 369, 373.

21 Ibid; *Loughnan (Principal Registrar, Family Court of Australia) v Altman* (1992) 111 ALR 445.

22 *Davison v Commonwealth* [1998] FCA 529.

23 *Re O'Sullivan and the Family Court of Australia* (1997) 47 ALD 765.

Examples of exempt activities	**Examples of activities covered by the *Privacy Act***
Research for the writing of judgments Draft judgments Pleadings Witness statements Documents obtained through return of summons Affidavits Unrevised and unpublished transcripts of proceedings Documents relating to pre-trial and settlement conferences Documents relating to ADR work performed by court staff[24]	Payroll records Employment records of court staff Documents concerning the court's contractors and suppliers Documents relating to the court's property management

35.13 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC did not propose any change to the exemption of federal courts from the operation of the *Privacy Act*. The ALRC observed that the partial exemption of federal courts is premised on the doctrine of separation of powers as well as the principle of open justice. While acknowledging the inherent difficulty in distinguishing between judicial and administrative matters, the ALRC noted that there already is a line of established jurisprudence in the context of the FOI Act. The ALRC considered that federal courts should continue to be exempt from the operation of the *Privacy Act*, except in respect of matters of an administrative nature.

Submissions and consultations

35.14 One stakeholder supported a total exemption of federal courts from the operation of the *Privacy Act*

> on the basis that the Courts themselves, either individually or collectively, would maintain a regime for protecting individuals' privacy as well as access to their records

24 For court-referred ADR processes that are conducted by external ADR practitioners, see Ch 44.

> in appropriate cases through rules of court. This would provide federal courts with the flexibility to amend the rules to maintain the balance with the increasing take up by courts of technology, such as online filing, access through the internet to individual court records etc. Were it considered necessary to establish a common statutory framework for the regulation of information privacy in federal courts, appropriate provisions could be inserted directly into the relevant Acts of Parliament.[25]

35.15 Some stakeholders supported the retention of the partial exemption that applies to the federal courts.[26] It was accepted that the doctrine of separation of powers and the principle of open justice are key principles underpinning the exemption,[27] and that the exemption reflects an appropriate balance between openness and the privacy needs of individuals.[28] The Right to Know Coalition submitted that the exemption is necessary to ensure that the public can be informed of the activities of the judiciary through media reports, and that the media's ability to report effectively on court proceedings is dependent on its ability to have proper access to court records and proceedings. It stated that it would strongly oppose any proposal to remove the exemption 'as this would severely undermine the media's ability to continue to report to the public on court proceedings'.[29]

35.16 Several stakeholders submitted that the *Privacy Act* may not be the appropriate instrument for resolving privacy concerns about court records and proceedings, and that the regulation of access to court records should be left to other legislation or procedural directives.[30] For example, the Centre for Law and Genetics stated that, while the lack of national consistency is problematic, it should be left to other legislation to impose restrictions on access to court documents and hearings.[31] The Office of the Privacy Commissioner (OPC) suggested that 'changes to court record publication are best dealt with through procedural directives or guidelines rather than legislative intervention'.[32]

35.17 Both the Legal Aid Commission of New South Wales and the Mental Health Legal Centre, however, expressed concerns about instances where sensitive information was obtained from judgment databases or disclosed in court.[33] These

---

25 Confidential, *Submission PR 214*, 27 February 2007.

26 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Right to Know Coalition, *Submission PR 542*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

27 Right to Know Coalition, *Submission PR 542*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

28 Confidential, *Submission PR 214*, 27 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007.

29 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

30 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Confidential, *Submission PR 214*, 27 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

31 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

32 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

33 Mental Health Legal Centre Inc, *Submission PR 184*, 1 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

include: spent convictions in judgment databases being used to harass the individuals concerned;[34] psychiatric reports being read in open court by a magistrate; and details of a woman's identity and mental health information being released to the press in the Coroners Court in Victoria.[35]

35.18 There were opposing views as to whether the current distinction between administrative and non-administrative matters should be maintained. Noting the difficulties in distinguishing between adjudicative and administrative functions, the Cyberspace Law and Policy Centre was nevertheless supportive of retaining the exemption. It argued that 'there is an established jurisprudence around the same distinction in the FOI Act'.[36]

35.19 Another stakeholder argued that the distinction between administrative and non-administrative matters is unsatisfactory because every activity undertaken by the courts by way of administration is undertaken for the sole purpose of serving and supporting judicial officers in the exercise of judicial power. It was suggested that, if the Act were to continue to apply to courts and tribunals, the distinction between administrative and non-administrative matters should be clarified through a non-exhaustive definition.[37]

35.20 The National Alternative Dispute Resolution Advisory Council (NADRAC) submitted that it is unclear to what extent the exemption applies to court-provided, court-ordered or court-referred ADR processes. It noted that, while 'ADR is not intrinsically a judicial function … it may be regarded as being an exercise of judicial power'. Judicial settlement conferences conducted by judicial officers and quasi-judicial officers are an example. In addition, NADRAC pointed out that 'ADR is frequently integrated into the judicial process without necessarily being an exercise of judicial power', for example, where courts referred matters to approved external ADR practitioners.[38]

Options for reform

35.21 The current exemption for federal courts was generally supported. What is at issue is the difficulty in distinguishing between activities of the court that relate to 'a matter of an administrative nature', which is covered by the *Privacy Act*, and those activities that do not relate to such matters and therefore are exempt from the operation of the Act. To clarify this distinction, the ALRC considered the following options for reform in DP 72.

---

34 Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.
35 Mental Health Legal Centre Inc, *Submission PR 184*, 1 February 2007.
36 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
37 Confidential, *Submission PR 377*, 5 December 2007.
38 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008.

35.22 One option would be to couch the exemption in positive terms, that is, exempting federal courts from the operation of the *Privacy Act* in respect of their judicial functions. This is the approach taken in New Zealand, New South Wales and the Northern Territory.[39]

35.23 Another option would be to exempt federal courts in respect of their judicial and quasi-judicial functions. This is the approach used in Victoria and Tasmania.[40] The term 'quasi-judicial function', however, is imprecise and may not be significantly different from a function that is 'truly ancillary to an adjudication by the court'.

35.24 A third option would be either to define the word 'administrative' or the word 'judicial'. For example, the *Privacy and Personal Information Protection Act 1998* (NSW) provides that the 'judicial functions of a court' means:

> the functions of the court … as relate to the hearing or determination of proceedings before it, and includes:
>
> (a) in relation to a Magistrate—such of the functions of the Magistrate as relate to the conduct of committal proceedings, and
>
> (b) in relation to a coroner—such of the functions of the coroner as relate to the conduct of inquests and inquiries under the *Coroners Act 1980*.

35.25 One definition suggested is that:

> anything done for or in relation to the exercise of judicial power, or making arrangements for the exercise of judicial power or a court event, whether by a judge, under the control of or delegation by a judge or judges, or by a member of the staff of the court or otherwise, is not taken as administrative. This would include anything in relation to case management, listings, steps taken in the course of a proceeding or pending proceeding under order and like matters.[41]

35.26 Finally, the exemption could be clarified by stating that federal courts are exempt from the operation of the *Privacy Act* except in relation to matters concerning their office administration. Although the term 'office administration' is not used in other legislation, it serves to clarify that it is matters unrelated to proceedings before the court that are intended to be covered by the *Privacy Act*, including corporate services, contracts, human resources, information technology, building operations and facilities, and finance.

ALRC's view

35.27 The partial exemption of federal courts from the operation of the *Privacy Act* is based on two fundamental principles underpinning Australia's system of government: the doctrine of separation of powers and the principle of open justice. The doctrine of

---

39 *Privacy Act 1993* (NZ) s 32(1) (definition of 'agency'); *Privacy and Personal Information Protection Act 1998* (NSW) s 6; *Information Act 2002* (NT) ss 4 (definition of 'tribunal'), 5(5)(a).

40 *Information Privacy Act 2000* (Vic) s 10; *Personal Information Protection Act 2004* (Tas) s 7(a), (b).

41 Confidential, *Submission PR 377*, 5 December 2007.

the separation of powers is embodied in the *Australian Constitution* to prevent the concentration of power on any one branch of government. It also was intended to avoid interference with the independence of the judiciary and to foster the proper administration of justice.[42] Requiring federal courts to comply with the *Privacy Act* in the exercise of their judicial functions would expose them to administrative review of their judicial activities, which would be inconsistent with the separation of judicial and executive arms of government.

35.28 The principle of open justice is the common law principle that justice should be administered in open court to ensure the fair and impartial administration of justice.[43] The disclosure of personal information in open court, however, is in direct conflict with the interests of privacy. While there should be an appropriate balance between the interests of privacy and the principle of open justice, the need to ensure the separation of judicial power means that the *Privacy Act* is not the appropriate mechanism to deal with matters relating to the courts' exercise of judicial powers. Accordingly, the partial exemption of federal courts from the operation of the *Privacy Act* should be retained. In the exercise of their judicial functions, it is appropriate for federal courts to deal with the handling of personal information in their own procedural rules.

35.29 Federal courts should, however, continue to be bound by the *Privacy Act* in respect of matters of an administrative nature. While the ALRC acknowledges the inherent difficulty in distinguishing between judicial and administrative matters, it is not a reason for exempting federal courts entirely from the operation of the Act. Given that the partial exemption of the courts is based in part on the separation of powers, there is no justification for exempting the courts in respect of their administrative operations.

35.30 The nature of matters to be classified as 'administrative' or 'non-administrative' does not lend itself to legislative definition. Although the term 'a matter of an administrative nature' causes difficulties in interpretation, any alternative definition would raise similar problems concerning the scope of the exemption. For example, defining 'administrative' to exclude 'anything done or in relation to the exercise of judicial power, or making arrangements for the exercise of judicial power or a court event' would be too wide and would raise the same issues concerning interpretation.

---

42 See, eg, D Williams, 'Judicial Power and Good Government' (2000) 11(2) *Public Law Review* 133 , 133.

43 *Scott v Scott* [1913] AC 417; *Dickason v Dickason* (1913) 17 CLR 50; *Russell v Russell* (1976) 9 ALR 103.

Federal tribunals

Background

35.31 Except for the Australian Industrial Relations Commission (AIRC), federal tribunals are not exempt from the operation of the *Privacy Act*. Before considering whether they should be exempt, the threshold issue is which agencies fall within the term 'federal tribunal'. This issue arises because the term 'tribunal' is imprecise and difficult to define.[44] Some legislative attempts at defining tribunals do not distinguish tribunals from courts. For example, the *Legislation Act 2001* (ACT) defines tribunal to include 'any entity that is authorised to hear, receive and examine evidence'.[45] Other definitions distinguish 'tribunal' from courts, but do not distinguish it from other review agencies, such as ministers and other public decision makers. For example, s 2 of the *Administrative Law Act 1978* (Vic) provides that:

> ***tribunal*** means a person or body of persons (not being a court of law or a tribunal constituted or presided over by a Judge of the Supreme Court) who, in arriving at the decision in question, is or are by law required, whether by express direction or not, to act in a judicial manner to the extent of observing one or more of the rules of natural justice.

35.32 The Council of Australasian Tribunals (COAT), the peak body for all Commonwealth, state, territory and New Zealand tribunals,[46] defines 'tribunal' as:

> any Commonwealth, State, Territory or New Zealand body whose primary function involves the determination of disputes, including administrative review, party/party disputes and disciplinary applications but which in carrying out this function is not acting as a court.[47]

35.33 One way of categorising tribunals is to divide them into 'court-substitute' and 'policy-oriented' tribunals. Court-substitute tribunals are closely modelled on courts and primarily act as providers of dispute resolution services. Tribunals that are considered to be court-substitute tribunals are merits review tribunals, such as the Administrative Appeals Tribunal (AAT), and those that have taken over former jurisdictions of the courts, such as consumer claims tribunals. Policy-oriented tribunals, such as the Australian Communications and Media Authority and Australian Security and Investment Commission, are mainly responsible for formulating and applying policy, but may have adjudicative and other functions.[48] In practice, however, the division between policy and court-substitute tribunals is not strict.

---

44 M Groves and H Lee, *Australian Administrative Law—Fundamentals, Principles and Doctrines* (2007), 78; C Enright, *Federal Administrative Law* (2001), 33.

45 *Legislation Act 2001* (ACT) sch 1.

46 Council of Australasian Tribunals, *About the Council of Australasian Tribunals* <www.coat.gov.au/overview.htm> at 1 May 2008.

47 Council of Australasian Tribunals Inc, *Constitution of the Council Of Australasian Tribunals Inc*.

48 M Allars, *Introduction to Australian Administrative Law* (1990), 312–313.

35.34 There is no exhaustive list of federal tribunals. COAT currently has 13 members that are federal tribunals, including: the AAT; the Australian Competition Tribunal; the Classification and Review Board; the Companies Auditors and Liquidators Disciplinary Board; the Copyright Tribunal of Australia; the Migration Review Tribunal; the Refugee Review Tribunal; the National Native Title Tribunal; the OPC; the Professional Services Review scheme; the Social Security Appeals Tribunal; the Superannuation Complaints Tribunal; and the Veterans' Review Board.[49] Membership with COAT is voluntary, however, and many federal tribunals are not members of the body.[50]

35.35 Since federal tribunals are part of the executive arm of government, they are prohibited from exercising the judicial power of the Commonwealth under s 71 of the *Australian Constitution*.[51] They lack the power to make determinative findings of law, and their decisions are subject to scrutiny by the courts, either through judicial review or statutory appeal on questions of law. The decision-making powers of tribunals are drawn from, and cannot exceed, those of the primary decision maker. Tribunals only may interpret law incidentally in the course of their proceedings, and such interpretations are not binding on the parties as a declaration of rights and obligations.[52] They also have no power to enforce their own decisions.[53]

Application of the IPPs to federal tribunals

35.36 Federal tribunals are currently able to rely on the exceptions to Information Privacy Principles (IPPs) 10 and 11 to use and disclose personal information in the course of exercising their functions.[54] IPPs 10 and 11 relevantly provide that an agency may use or disclose personal information where:

- the individual is aware, or reasonably likely to be aware, that information of that type is usually passed to a person, body or agency;[55]
- the individual has consented to the use or disclosure; [56]

---

49 Council of Australasian Tribunals, *Register of Tribunals* <www.coat.gov.au/register.htm> at 1 May 2008.

50 For example, the Defence Force Discipline Remuneration Tribunal, the Defence Force Discipline Appeal Tribunal, the Federal Police Disciplinary Tribunal, the Repatriation Commission and the Pharmaceutical Benefits Remuneration Tribunal.

51 *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254.

52 *Re Cram; Ex parte The Newcastle Wallsend Coal Company Pty Ltd* (1987) 163 CLR 140, 149.

53 A Hall, 'Judicial Power, the Duality of Functions and the Administrative Appeals Tribunal' (1994) 22 *Federal Law Review* 13, 55.

54 *Privacy Act 1988* (Cth) s 14, IPPs 10, 11; Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007; Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007.

55 *Privacy Act 1988* (Cth) s 14, IPP 11.1(a).

56 Ibid s 14, IPPs 10.1(a), 11.1(b).

- the record-keeper believes on reasonable grounds that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or other persons; [57]

- use or disclosure is required or authorised by or under law; [58]

- use or disclosure is reasonably necessary for enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue;[59] or

- use of the information is directly related to the purpose for which it was obtained.[60]

35.37 In addition, the constituent Acts of these tribunals authorise the use and disclosure of personal information in certain situations.

Industrial tribunals

35.38 Agencies listed in sch 1 of the FOI Act are exempt from the *Privacy Act* except in relation to administrative matters.[61] These agencies include the AIRC and the Industrial Registrar and Deputy Industrial Registrars. Another agency listed in sch 1 of the FOI Act is the Australian Fair Pay Commission (AFPC). The AFPC is not a tribunal.[62] The exemption that applies to the AFPC is considered in Chapter 36.

35.39 The AIRC is an independent, national industrial tribunal established under the *Workplace Relations Act 1996* (Cth). The functions of the AIRC include: assisting employers and employees in resolving industrial disputes; handling certain termination of employment claims; rationalising and simplifying awards; and dealing with applications about industrial action.[63] The Industrial Registrar and Deputy Registrars provide administrative support to the AIRC. They also have responsibilities relating to the registration of unions and employer associations and their financial accountability.[64]

35.40 In performing its functions, the AIRC has certain powers, including the power to: inform itself in any manner it thinks appropriate; take evidence on oath or affirmation; conduct proceedings in private; summons any person to be present before

---

57 Ibid s 14, IPPs 10.1(b), 11.1(c).
58 Ibid s 14, IPPs 10.1(c), 11.1(d).
59 Ibid s 14, IPPs 10.1(a), 11.1(e).
60 Ibid s 14, IPP 10.1(e).
61 Ibid s 7(1)(a)(i)(A), (b).
62 The AFPC is an independent, statutory body that is responsible for setting and adjusting federal minimum wages: *Workplace Relations Act 1996* (Cth) s 23.
63 Ibid s 62; Australian Industrial Relations Commission, *About the Commission* <www.airc.gov.au> at 5 August 2007.
64 Australian Industrial Relations Commission, *About the Commission* <www.airc.gov.au> at 5 August 2007.

the AIRC; compel the production of documents and other things; direct a person to attend a conference; and make interim and final decisions.[65]

Other federal tribunals

35.41 Other than the AIRC, no federal tribunals are exempt from the operation of the *Privacy Act*. Some examples of federal tribunals include the AAT, the Migration Review Tribunal (MRT), the Refugee Review Tribunal (RRT), the Social Security Appeals Tribunal (SSAT) and the National Native Title Tribunal (NNTT).

Administrative Appeals Tribunal

35.42 The AAT provides independent review of a wide range of administrative decisions made by the Australian Government and some non-government bodies. The AAT has jurisdiction to review decisions made under more than 400 separate Acts and legislative instruments, including decisions in the areas of social security, taxation, veterans' affairs, workers' compensation, bankruptcy, civil aviation, corporations law, customs, freedom of information, immigration and citizenship, industry assistance and security assessments undertaken by the Australian Security Intelligence Organisation.[66]

35.43 The AAT generally is required to hold hearings in public, except where the AAT is satisfied that, by reason of the confidential nature of any evidence or matter or for any other reason, it is desirable for the hearing to be held in private.[67] The AAT may give directions prohibiting or restricting the: publication of the names and addresses of witnesses; publication of matters contained in documents lodged with, or received in evidence by, the AAT; and the disclosure to some or all of the parties of evidence given before the AAT, or of the content of a document lodged with, or received in evidence by, the AAT.[68] In addition, an application for a review of a security assessment made to the Security Appeals Division of the AAT must be held in private.[69] The AAT also may restrict the publication of evidence and findings in the hearing of such an application.[70] The AAT is required to give reasons either orally or in writing for its decision, except in limited circumstances.[71]

35.44 Members and staff of the AAT are subject to a number of provisions prohibiting the disclosure of information in particular circumstances. These confidentiality

---

65 *Workplace Relations Act 1996* (Cth) ss 111, 115.
66 Administrative Appeals Tribunal, *About the AAT* <www.aat.gov.au/AboutTheAAT.htm> at 14 May 2008.
67 *Administrative Appeals Tribunal Act 1975* (Cth) s 35.
68 Ibid s 35(2).
69 Ibid s 39A(1).
70 Ibid s 35AA.
71 Ibid s 28.

obligations are found in the *Administrative Appeals Tribunal Act 1975* (Cth) and in other Acts and legislative instruments that confer jurisdiction on the AAT.[72]

Migration Review Tribunal and Refugee Review Tribunal

35.45 The MRT is a merits review body established under the *Migration Act 1958* (Cth). The MRT provides a final, independent merits review of visa and visa-related decisions made by the Minister for Immigration and Citizenship or, more typically, by officers of the Department of Immigration and Citizenship, acting as delegates of the Minister.[73] The MRT must conduct hearings in public, unless the tribunal considers that it is in the public interest to take evidence in private.[74] Examples of matters where an MRT review may be conducted in private include cases that involve allegations of children at risk of domestic violence, or sensitive information about the health of an individual.[75]

35.46 The RRT also was established under the *Migration Act*. It is an independent merits review tribunal, responsible for reviewing decisions made by the Department of Immigration and Citizenship to refuse or cancel protection visas to non-citizens in Australia. The RRT also has the power, in respect of certain 'transitory persons', to conduct an assessment of whether a person falls within the legal meaning of 'refugee'.[76] Unlike a court, the RRT is not adversarial. The Department usually is not represented at RRT hearings. The RRT is inquisitorial in nature and can obtain whatever information it considers necessary to conduct the review. All reviews before the RRT must be conducted in private.[77]

35.47 Both the MRT and RRT are subject to the same confidentiality requirements under the *Migration Act*. Sections 377 and 439 of the Act prohibit members and officers of the tribunals and interpreters from recording, communicating or divulging any information or documents about a person obtained in the course of exercising a function or duty under the Act, unless it is necessary for the performance of that function or duty or for the purposes of the Act. In addition, both tribunals have the power to restrict publication of information if it is in the public interest to do so.[78]

Social Security Appeals Tribunal

35.48 The SSAT is a statutory body established under the *Social Security (Administration) Act 1999* (Cth). It falls within the portfolio of the Minister for Families, Housing, Community Services and Indigenous Affairs. The role of the SSAT

---

72 See, eg, Ibid ss 66, 66A.

73 Australian Government Migration Review Tribunal and Refugee Review Tribunal, *About the Tribunals* <www.mrt-rrt.gov.au/about.asp> at 15 May 2008.

74 *Migration Act 1958* (Cth) s 365.

75 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126*, 16 January 2007.

76 *Migration Act 1958* (Cth) s 411. A 'transitory person' is a person who has been in Australia for 6 months or more: *Migration Act 1958* (Cth) s 5.

77 *Migration Act 1958* (Cth) s 429.

78 Ibid ss 378, 440.

is to conduct merits review of administrative decisions made under social security law, family assistance law, child support law and various other pieces of legislation. It is the first level of external review of decisions made by Centrelink about social security, family assistance, education or training payments. It is also the first level of external review of most decisions made by the Child Support Agency.[79]

35.49 The SSAT must hear reviews in private, and directions may be given as to the persons who may be present at any hearing of a review. In giving such directions, the wishes of the parties and the need to protect their privacy must be considered.[80] The Executive Director of the SSAT may make an order directing a person who is present at the hearing not to disclose information obtained in the course of the hearing.[81] When the SSAT makes its decision on a review, it must prepare a written statement setting out the decision, the reasons for the decision and the findings on any material questions of fact, and refer to evidence and other materials on which the findings of fact were based.[82] A copy of the statement must be given to the parties to the review.[83] Members of the tribunals and interpreters are prohibited from recording, communicating or divulging any information or documents about a person obtained in the course of exercising a function or duty under the Act, unless it is necessary for the performance of that function or duty or for the purposes of the Act.[84]

National Native Title Tribunal

35.50 The NNTT is an independent Australian Government agency established under the *Native Title Act 1993* (Cth) to assist people to resolve native title issues over land and water. It falls under the portfolio of the Attorney-General of Australia.[85]

35.51 The NNTT has numerous functions, including: holding inquiries in relation to native title issues and applications; holding mediation conferences concerning native title claims; reviewing whether a native title claim group holds native title rights and interests; reconsidering native title claims where the Native Title Registrar does not accept a native title claim for registration; providing assistance, mediating or conducting reviews; making determinations or making a report after holding certain inquiries; and carrying out research for the purpose of performing its functions.[86]

---

79 Australian Government Social Security Appeals Tribunal, *Introduction to the SSAT* <www.ssat.gov.au> at 15 May 2008.
80 *Social Security (Administration) Act 1999* (Cth) s 168.
81 Ibid s 169.
82 Ibid s 177.
83 Ibid s 177.
84 Ibid s 19.
85 National Native Title Tribunal, *About the Tribunal* <www.nntt.gov.au/Pages/default.aspx> at 1 May 2008.
86 *Native Title Act 1993* (Cth) s 108.

35.52 For the purposes of an inquiry, the President of the NNTT may direct the holding of a conference of the parties or their representatives to help resolve any matter that is relevant to the inquiry or hearings. The NNTT has the power to take evidence on oath or affirmation; summon a person to appear before it to give evidence and produce documents; receive evidence in the course of an inquiry and draw conclusions of fact from the transcript of evidence in proceedings; adopt any report, findings, decision, determination or judgments that may be relevant to an inquiry; and dismiss applications or reinstate applications that have been dismissed in error.[87]

35.53 The NNTT must hold mediation conferences in private, unless the presiding member directs otherwise and no party objects.[88] On the other hand, hearings conducted for the purposes of an inquiry are to be held in public except in certain circumstances.[89] Reviews, mediation conferences and conferences held for the purposes of an inquiry are made without prejudice to the parties' legal rights.[90] The presiding member of an inquiry or review may prohibit the disclosure of information given, statements made or contents of documents produced at a conference or in the course of a review of native title rights and interests.[91] The NNTT also may prohibit the disclosure of any evidence given before it or the contents of any documents produced to it during hearings.[92] Determinations and reports about matters covered in an inquiry must be in writing and must state any findings of fact upon which the determination or report is based.[93]

Submissions and consultations

35.54 In DP 72, the ALRC asked whether the *Privacy Act* should be amended to provide that federal tribunals be exempt from the operation of the Act in respect of their adjudicative functions; and if so, what the scope of 'adjudicative functions' should be.[94]

Industrial tribunals

35.55 The President of the AIRC, the Hon Justice GM Giudice, submitted that the AIRC should remain exempt from the operation of the *Privacy Act* for two main reasons: the AIRC is obliged to act judicially; and, subject to some exceptions, its hearings and decisions are open to public scrutiny. His Honour stated that the policy issues that apply to the courts also apply to bodies that are required to act judicially, and therefore the AIRC should be in the same position as the courts.[95]

---

87 Ibid ss 149, 149A, 156.
88 Ibid s 136E.
89 Ibid ss 154, 154A.
90 Ibid ss 136A, 136GC, 150.
91 Ibid ss 136F, 136GD.
92 Ibid ss 155.
93 Ibid ss 162, 163, 163AA, 163A, 164.
94 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 32–1.
95 Justice G Giudice, *Submission PR 91*, 15 January 2007.

35.56 The Department of Employment and Industrial Relations (DEWR) (now the Department of Education, Employment and Workplace Relations) submitted that, on public interest grounds, the industrial tribunals should remain exempt in relation to non-administrative matters. DEWR suggested that:

> These organisations are not exempt in relation to their administrative activities, only in connection with their official functions. In this regard, these standard setting, conciliation and quasi-judicial tribunals are treated in the same fashion as federal courts … and DEWR is not aware of any compelling arguments to remove the exemption.[96]

35.57 While not commenting on whether the current partial exemptions that apply to industrial tribunals are appropriate, the OPC considered that 'entities with like functions should be treated consistently under the *Privacy Act*'. The OPC also suggested that 'where exemptions apply it would be worthwhile introducing good privacy practices so that individuals understand how their personal information will be handled'.[97]

35.58 One individual submitted that there is no valid reason why there should be an exemption for agencies in the area of industry and the workplace.[98]

Exemption for 'federal tribunals' as a class of agencies

35.59 The AAT and SSAT submitted that it may not be appropriate to exempt all federal tribunals,[99] particularly given the different objects and purposes of the FOI Act and *Privacy Act*,[100] and the fact that some of them are required to hold hearings in private.[101] In contrast, the MRT and RRT stated that, although they do not consider that there is a need for them to be exempt from the operation of the *Privacy Act*, they anticipate that 'consideration may be given by the ALRC to the degree to which there should be consistency in coverage in respect to all federal tribunals'.[102]

35.60 While not commenting on whether federal tribunals should be partially exempt from the operation of the *Privacy Act*, the OPC considered that 'entities with similar functions should be treated consistently' under the exemption provisions of the *Privacy Act*. It noted that, since the ALRC supports the use of the words 'non-administrative nature' in relation to federal courts, the same words should be used in framing any

---

96 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.
97 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
98 K Handscombe, *Submission PR 89*, 15 January 2007.
99 Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007; Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007.
100 Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007.
101 Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007.
102 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126*, 16 January 2007.

exemption that applies to federal tribunals so as to promote consistency. The OPC submitted that, if the exemptions that apply to courts and tribunals are framed differently, the policy basis for such a difference should be explained. The OPC further stated that:

> Whichever form of words is used, the Office submits the exemption should be clearly defined so as to enable agencies, organisations and the community to determine what information falls within the scope of an exemption.[103]

35.61 Both the Australian Privacy Foundation and the Cyberspace Law and Policy Centre submitted that there should be no general exemptions for federal tribunals, as they appear to operate effectively despite being subject to the IPPs.[104]

35.62 Some stakeholders submitted that a limited exemption or specific exceptions to the privacy principles would be more appropriate in relation to federal tribunals. The Public Interest Advocacy Centre (PIAC) accepted that compliance with privacy principles may cause difficulties for tribunals in some circumstances, for example, where tribunals need to disclose personal information for the purposes of their review functions. It considered, however, that there is no justification for a broad exemption for federal tribunals. Instead, such difficulties should be dealt with by way of specific, limited exceptions to the privacy principles.[105]

35.63 National Legal Aid also saw value in 'a more limited exemption to cover adjudicative functions', but questioned whether this should take the form of 'a blanket exemption from the proposed uniform privacy principles or could be practically achieved by an appropriate exemption from those principles which do not fit with adjudicative functions'.[106]

35.64 Privacy NSW noted that an exemption for federal tribunals in respect of their adjudicative functions would be consistent with the exemption that applies to federal courts as well as that which applies to New South Wales courts and tribunals under New South Wales privacy law. It submitted, however, that 'consistency is not necessarily a compelling policy reason' for granting federal tribunals an exemption. Privacy NSW suggested that:

> should federal tribunals be exempted, they should, (along with federal courts and other tribunals), develop and publish privacy rules that form part of the court or tribunal procedural rules. Such rules should include guidance to judges and tribunal members about limiting the inclusion of sensitive or high value identification information in judgements, especially those which will be published electronically.[107]

---

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

104 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

105 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

107 Privacy NSW, *Submission PR 468*, 14 December 2007.

35.65 One stakeholder noted that 'there is not the same constitutional basis for exempting tribunals as exists in the case of Courts'. It nevertheless supported the exemption of tribunals from the operation of the *Privacy Act* in the performance of their adjudicative functions. This is because the integrity of the adjudicative process requires that a review of, or an appeal against, a tribunal's decision only should be brought in the manner for which its enabling legislation provides. Subjecting a tribunal's decision to a review by the OPC would allow litigants to seek a secondary review of that decision outside of the adjudicative process.[108]

35.66 The Australian Bankers' Association submitted that 'the widespread use of tribunals instead of courts for the resolution of cases ought to place tribunals in a position comparable with the courts'.[109]

35.67 NADRAC submitted that, whether court-provided, court-ordered or court-referred, ADR processes fell within the scope of the exemption of federal courts from the operation of the *Privacy Act*. It suggested that the issue of whether ADR processes are clearly within the scope of an exemption is equally relevant to tribunals, which are significant providers and users of ADR, as it is to courts.[110]

Exemption for individual tribunals

35.68 In their submissions, several tribunals argued that they should be partially exempt from the operation of the *Privacy Act*. The AAT considered that it should be exempt in the same way as federal courts in the interests of consistency and in accordance with the principle of open justice.[111] The AAT argued that it should be exempt 'in relation to activities undertaken for the purpose of carrying out its functions under the *Administrative Appeals Tribunal Act 1975*', for the following reasons:

- as a body that resolves disputes, the AAT shares significant attributes with the federal courts, which are partially exempt from the *Privacy Act*, and with courts and tribunals that are partially exempt from privacy legislation in a number of states and territories;

- there is extensive overlap between the work of the Federal Court and that of the AAT, and the AAT is quite distinct from other federal tribunals because it acts like a court;

---

108 Confidential, *Submission PR 377*, 5 December 2007.
109 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.
110 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008.
111 Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007.

- privacy issues are already dealt with appropriately by the AAT within the framework of the AAT Act, as well as through consultation with the Privacy Commissioner; and

- the application of a number of the proposed Unified Privacy Principles (UPPs) would present difficulties for the AAT. The AAT would have to rely extensively on exceptions to the UPPs in the course of its ordinary operations, indicating that it would be appropriate for it to be partially exempt.[112]

35.69 In its submission to Issues Paper 31, *Review of Privacy* (IP 31), the SSAT stated that it should not be exempt from the operation of the *Privacy Act*, on the proviso that the exceptions to privacy principles concerning the use and disclosure of personal information remain substantially the same.[113]

35.70 The MRT and RRT also have previously submitted that there was no need for them to be exempt from the operation of the *Privacy Act*, on the basis that exceptions to the IPPs would permit the tribunals to disclose personal information where it is necessary for the purposes of a particular review.[114] While the MRT and RRT remained of the view that an exemption from the *Privacy Act* in its current form is not required, they submitted that an exemption in respect of their adjudicative functions would be appropriate if the UPPs were to be adopted.[115]

35.71 The AAT, SSAT, MRT and RRT also submitted that their legislative framework provides an appropriate level of safeguards for their handling of personal information, including requirements under different pieces of legislation,[116] and confidentiality obligations on tribunal staff prohibiting disclosure of information in particular circumstances.[117]

35.72 The NNTT submitted that there should be a specific exception in relation to its research function in support of resolving native title claims.

> Research undertaken in performance of this function may result in the collection of personal information from publicly available sources and from unpublished materials. Obtaining consent to disclose personal information in NNTT research materials for

---

112 Ibid.

113 Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007. In response to DP 72, the SSAT submitted that its previously stated view was predicated on the assumption that the Act would remain substantially the same. The SSAT submitted that, given the proposed UPPs, it would need to read the UPPs in light of the SSAT's own legislative requirements and obligations, and may seek partial exemptions from the operation of specific UPPs: Social Security Appeals Tribunal, *Submission PR 478*, 17 December 2007.

114 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126*, 16 January 2007.

115 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 533*, 21 December 2007.

116 Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007; Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126*, 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106*, 15 January 2007.

117 Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007; Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126*, 16 January 2007.

> NNTT mediation of native title applications is so onerous as not to be possible in some cases and not practicable in others.[118]

35.73 The NNTT suggested that the exception could be based on a similar exception under either: the 'Collection' principle in the model UPPs, which allows for the collection of personal information where it 'is necessary for the establishment, exercise, or defence of a legal or equitable claim'; or s 8(2)(k) of the *Privacy Act 1985* (Canada), which permits disclosure of personal information 'for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada'.[119]

ALRC's view

35.74 One argument for exempting federal tribunals from the operation of the *Privacy Act* is that they have to rely heavily on exceptions to privacy principles in the course of their ordinary operations. That, however, does not provide a sufficient justification for exempting federal tribunals from the operation of the Act. As explained in Chapter 4, privacy principles are designed to be relatively high-level statements of policy objectives. This enables the principles to apply flexibly in a myriad of different information-handling contexts. It is to be expected that some agencies have to rely on the exceptions built into the principles in specified situations or in respect of certain conduct. In any case, federal tribunals currently rely on existing exceptions in the IPPs. Similar exceptions are retained in the model UPPs.[120]

35.75 The main argument in favour of exempting federal tribunals is that they perform similar functions to the courts and therefore should be exempt to the same extent as courts. Not all of the rationales that apply to the exemption of federal courts, however, apply to federal tribunals. The partial exemption of federal courts from the operation of the *Privacy Act* is based partly on the need to balance the principle of open justice with the interests of privacy. The principle of open justice, however, does not apply equally to all federal tribunals. The extent to which the principle applies to a particular tribunal depends on the nature of the tribunal's jurisdiction and the tribunal's operating environment. The principle of open justice also does not always apply equally to all proceedings before a particular tribunal. For example, some tribunals generally are required to hold hearings in public, but are required to hold particular types of hearings in private. They also may have a discretion as to whether to hold hearings in public or in private.

---

118 National Native Title Tribunal, *Submission PR 402*, 7 December 2007.

119 Ibid.

120 For example, the NNTT, where it is carrying out its statutory research functions, would be able to rely on the 'required or authorised by or under law' exceptions in the 'Collection' and 'Use and Disclosure' principles in the model UPPs.

35.76 The partial exemption of federal courts also is based in part on the separation of powers in Chapter III of the *Australian Constitution*. This rationale does not apply to federal tribunals, which exercise executive rather than judicial power. Nevertheless, many tribunals have adjudicative functions that are similar to the judicial functions of courts.[121] The functions of a tribunal generally include: evaluating evidence; conducting hearings; defining or determining any legal rights; and in the context of administrative review, not confining its evidence to that used by the decision maker.[122] On this basis, there is a strong case for exempting court-substitute tribunals in relation to their adjudicative and review functions in order to maintain the integrity of their adjudicative and review processes.

35.77 The ALRC does not consider that exempting the federal tribunals in respect of their adjudicative functions would cover sufficiently the range of activities that ought to be exempt. For example, the AAT may conduct conferences with the parties or their representatives before the hearing, as well as ADR processes which are an integral part of the AAT's review process. The NNTT also holds mediation conferences and other conferences in the course of an inquiry relating to native title claims. It is unclear whether the term 'adjudicative functions' or other similar terms would capture all of these activities, which are part of the dispute resolution process.

35.78 Exempting the AAT 'in relation to activities undertaken for the purpose of carrying out its functions'[123] under its empowering legislation would be too wide a formulation. Arguably, all of the AAT activities, including those relating to its office administration, could be considered activities that are undertaken for the purpose of carrying out its functions.

35.79 Entities with like functions should be treated alike. As discussed above, federal courts should continue to be exempt from the operation of the *Privacy Act*, except when they are dealing with matters of an administrative nature. Federal tribunals whose primary functions involve dispute resolution, administrative review and disciplinary proceedings also should be exempt to the same extent.[124]

35.80 Since the basis for the exemption is the exercise of court-like functions by tribunals, the exemption only should apply to federal tribunals whose primary functions involve dispute resolution, administrative review and disciplinary applications, rather than to those whose main functions are to formulate and apply policy.

---

121 See R Creyke and J McMillan, *Control of Government Action: Text, Cases & Commentary* (2005), [3.2.28]–[3.2.29].

122 *Re Monger; Ex parte WMC Resources Pty Ltd* [2002] WASCA 129, [76].

123 Administrative Appeals Tribunal, *Submission PR 201*, 20 February 2007.

124 The categorisation of tribunals used to frame the exemption is based on the definition of 'tribunal' in the Constitution of COAT, discussed above: Council of Australasian Tribunals Inc, *Constitution of the Council Of Australasian Tribunals Inc*.

35.81 In Chapter 33, the ALRC recommends that the *Privacy Act* should be amended to set out in a schedule to the Act exemptions for specified, named agencies, organisations and entities. Where such agencies, organisations and entities are partially exempt, the schedule should specify the particular acts and practices that are exempt. In the interest of certainty, this schedule should list the specific tribunals, boards and commissions that are partially exempt and specify the extent of their exemption. The list would include, for example, the AAT, SSAT, MRT, RRT and the AIRC.

35.82 In Chapter 33, the ALRC also recommends that where an entity is exempt, completely or partially, from the operation of the *Privacy Act*, information-handling guidelines should be in place to ensure that personal information would be handled appropriately. The ALRC recommends that those federal tribunals, commissions and boards that are exempt partially from the operation of the *Privacy Act* should develop and publish information-handling guidelines that apply to their activities in respect of matters of a non-administrative nature.

Recommendation 35–1 The *Privacy Act* should be amended to provide that federal tribunals, boards and commissions whose primary functions involve dispute resolution, administrative review or disciplinary proceedings are exempt from the operation of the Act except in relation to an act done, or a practice engaged in, in respect of a matter of an administrative nature. The schedule to the Act setting out exemptions should list the specific tribunals, boards and commissions that are partially exempt and specify the extent of their exemption.

Recommendation 35–2 Those federal tribunals, commissions and boards that are partially exempt from the operation of the *Privacy Act* should develop and publish information-handling guidelines that apply to their activities in respect of matters of a non-administrative nature.

Access to court and tribunal records

Individuals' access and correction rights

35.83 In Chapter 29, the ALRC recommends that the 'Access and Correction' principle in the model UPPs provide that, if an agency holds personal information about an individual, the individual concerned is entitled to have access to that personal information, except to the extent that the agency is required or authorised to refuse to provide access under the applicable provisions of any law of the Commonwealth, including the FOI Act.[125]

125 Rec 29–2.

35.84 Access to, and correction of, personal information held by federal courts and tribunals would, therefore, continue to be subject to the FOI Act. The FOI Act, however, does not apply to any request for access to a document of a court; or a tribunal, authority or other body specified in sch 1 of the FOI Act, unless 'the document relates to matters of an administrative nature'.[126]

35.85 Under the ALRC's recommendations, therefore, where personal information does not relate to matters of an administrative nature held by a court or tribunal, authority or other body specified in sch 1 of the FOI Act, neither the *Privacy Act* nor the FOI Act provisions would apply. Access to the information, however, may be permitted, subject to court and tribunal rules. Where personal information relates to matters of an administrative nature, individual rights of access to, and correction of, personal information will be subject to the FOI Act.

Third party access to court and tribunal records

35.86 Where personal information relates to matters of an administrative nature, requests for access to personal information by third parties—that is, persons other than the individual to whom the information relates—will be subject to the 'Use and Disclosure' principle in the model UPPs, and to the rules of courts and tribunals.

35.87 Where personal information does not relate to matters of an administrative nature, requests for access to personal information by third parties will be governed primarily by court and tribunal rules. In the course of the Inquiry, a range of concerns regarding third party access to court and tribunal records were raised, and are discussed below.

Research access to court records

35.88 Particular concerns have been expressed in relation to access to court records for research purposes. Research access may be considered an aspect of open justice because 'research offers a more considered and sustained evaluation of the way courts operate'.[127] Currently, no federal court rules specifically address the issue of researchers' access to court records. Researchers who seek access to court records that are not publicly accessible will be required to seek leave of the court, and in some cases show that they have a proper interest in searching court records and inspecting court documents.[128]

35.89 The Family Court of Australia has a detailed policy relating to the granting of research access to court records. The policy contains a number of requirements, including: the preservation of confidentiality of information; obtaining informed consent from study participants; restriction of access to medical or other treatment records, or other client data collection systems, to qualified clinical investigators; and

---

126 *Freedom of Information Act 1982* (Cth) ss 5, 6.
127 C Puplick, 'Justice: Now Open to Whom?' (2002) 6 *Judicial Review* 95, 105.
128 See, eg, *Federal Magistrates Court Rules 2001* (Cth) r 2.08(2).

clearance from an appropriate and credible ethics committee for certain types of studies. Applications for research access are considered by the Family Court's Research Committee, which makes recommendations to the Chief Justice and the Chief Executive Officer of the Family Court on whether access to the court's resources should be granted.

35.90 In its discussion paper on access to court records, the County Court of Victoria proposed a detailed process for approval of academic or commercial research utilising court records.[129] In its report on access to court records, the New Zealand Law Commission recommended that there be a single entry point for all requests for access to court records by researchers, and that the process and criteria for considering all research proposals be articulated fully and published.[130]

Discussion Paper proposal

35.91 In DP 72, the ALRC observed that research contributes to the understanding and improvement of the court system. The ALRC expressed the view that research should be encouraged, provided there are sufficient safeguards in place to ensure the proper handling of personal information.

35.92 One way of ensuring that safeguards are in place is by developing and publishing a policy on access to court records for research purposes. The ALRC noted that although the Family Court already had such a policy, it was not available on the Court's website. Other federal courts have not published a written policy in relation to access to court records for research purposes. The ALRC therefore proposed that federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.[131]

Submissions and consultations

35.93 Some stakeholders expressed support for the ALRC's proposal for the development and publication of policies on granting access for research purposes to

---

129 County Court of Victoria, *Discussion Paper: Access to Court Records* (2005), [28]. The Court stated that it would consider feedback on the discussion paper from court users and the general public in preparing its draft policy on access to court records: County Court of Victoria, *2005–06 Annual Report* (2006), 8. A new privacy policy outlining the procedures followed by the Court regarding the disclosure of information held in its records was posted on the Court's website and took effect on 1 March 2008: County Court of Victoria, *Privacy* <www.countycourt.vic.gov.au> at 30 April 2008.

130 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), [8.40], Rec R27. The New Zealand Government has referred the report to the Justice and Electoral Select Committee of the New Zealand Parliament for inquiry: New Zealand Government, *Government Response to Law Commission Report on Access to Court Records* (2007).

131 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 32–1.

court records.[132] The OPC submitted that the development of such policies could facilitate research in the public interest, while providing appropriate privacy protection.[133] National Legal Aid supported the proposal

> as a means of encouraging research into legal service delivery and promoting the accountability of the court system, while maintaining the general exclusion of the courts' non-administrative functions.[134]

35.94 PIAC noted that 'the policy by the Family Court is particularly comprehensive and could serve as a model'.[135] The National Health and Medical Research Council (NHMRC) stated that it 'would be pleased to assist with the development of policies relating to access to health information contained in court records'.[136]

35.95 Some stakeholders expressed support for the ALRC's recommendation, in its report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98),[137] that the Standing Committee of Attorneys-General (SCAG) should order a review of federal, state and territory legislation and court and tribunal rules concerning non-party access to court records, with a view to promoting a national and consistent policy.[138] One stakeholder opposed the recommendation, stating that 'absolute uniformity between federal courts is neither achievable nor desirable'.[139]

35.96 Privacy NSW noted that responsibility for privacy has been transferred from the portfolio of the Attorney-General's Department to the Department of the Prime Minister and Cabinet. It therefore suggested that the review of court and tribunal rules should be referred to the Council of Australian Governments (COAG) instead.[140] In this regard, the ALRC has been informed that, under the new administrative arrangements,[141] SCAG will continue to be the body to consider information privacy issues.[142] SCAG, therefore, remains the appropriate body to order a review of court rules concerning non-party access to court records.

---

132 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; National Legal Aid, *Submission PR 521*, 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; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

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

135 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

136 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

137 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 7–1.

138 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Privacy NSW, *Submission PR 468*, 14 December 2007.

139 Confidential, *Submission PR 377*, 5 December 2007.

140 Privacy NSW, *Submission PR 468*, 14 December 2007.

141 See Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

142 Australian Government Attorney-General's Department, *Correspondence*, 12 February 2008.

ALRC's view

35.97 The principle of open justice is consistent with the promotion of research, given that research contributes to the understanding and improvement of the court system. Therefore, provided there are sufficient safeguards in place to ensure the proper handling of personal information, research should be encouraged.

35.98 One way of ensuring that safeguards are in place is by developing and publishing a policy on access to court records for research purposes. The Family Court already has such a policy, but it is not available on the court's website. Other federal courts have not published a written policy in relation to access to court records for research purposes. The ALRC recommends that federal courts that do not have such a policy should develop and publish one. Such policies should address issues concerning the privacy of court users, such as confidentiality, the need for informed consent by participants, restricted access to sensitive information, and approval by ethics committees where appropriate. The policies could be developed in consultation with bodies that have experience in dealing with the privacy of personal information, such as the OPC, and the NHMRC in relation to health information.

Recommendation 35–3 Federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.

Other third party access

Public access to court records

35.99 Court records may contain sensitive personal information such as criminal history, psychiatric and psychological reports, and other medical records. Information on court records relating to certain types of proceedings also may be particularly sensitive, for example, in family law, bankruptcy and criminal proceedings. In addition, children are considered to be particularly vulnerable and therefore the identification of children in court records raises specific privacy concerns.[143]

35.100 Although exempt from the *Privacy Act*, access to documents on file in court registries is regulated by other statutes or rules of court.[144] In the High Court, any person may inspect and take a copy of any document filed in the registry except: affidavits and exhibits to affidavits that have not been received in evidence in court; and documents that contain identifying information about a person where the

143 The identification of children in court records is discussed in Ch 69.
144 *High Court Rules 2004* (Cth) r 4.07.4.

disclosure of the identity of that person is prohibited by an Act, an order of the court or otherwise.[145]

35.101 In the Federal Court, a person can search and inspect documents specified in the *Federal Court Rules 1979* (Cth)—such as applications, pleadings, judgments, orders and submissions—unless the court or a judge has ordered that the document is confidential.[146] A person who is not a party to the proceeding may inspect certain other documents only with the leave of the court.[147] Leave will usually be granted, however, where a document has been admitted into evidence or read out in open court.[148]

35.102 In the Federal Magistrates Court, only specified persons may search or inspect the court's records without leave granted by the court or the registrar. Records relating to a family law or child support proceeding only may be searched or inspected by the Attorney-General, and other records related to a particular proceeding only may be searched or inspected by the parties, their lawyers or a child representative in the proceedings. Leave to search or inspect a record may be granted to a person only if he or she can demonstrate a 'proper interest'.[149]

35.103 In the Family Court, only specified persons may search, inspect or copy the court's records relating to a case without the permission of the court. The specified persons include: the Attorney-General, the parties and their lawyers, and independent children's lawyers. Permission to search, inspect or copy a court record may be granted to a person with a 'proper interest' in the case or the information in that particular court record.[150]

35.104 Access to court records may be affected by the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth). The Act enables information to be introduced during federal criminal and civil proceedings in an edited and summarised form to facilitate the hearing of a case without prejudicing national security and the right of the defendant to a fair trial. A court exercising federal jurisdiction must hold closed hearings in certain circumstances,[151] and must not make a record of the hearing available to, or allow the record to be accessed by, anyone except specified persons or entities. The specified persons and entities include: the court hearing the appeal or reviewing the lower court's decision; the prosecutor in a criminal proceeding; the defendant's legal representative; an unrepresented party or a party's legal representative—provided that he or she has been given a security clearance at an

145 Ibid r 4.07.4.
146 *Federal Court Rules 1979* (Cth) o 46 r 6(1), (2).
147 Ibid o 46 r 6(3)–(5).
148 Federal Court of Australia, *Public Access to Court Documents* <www.fedcourt.gov.au/courtdocuments/publicdocuments.html> at 1 May 2008.
149 *Federal Magistrates Court Rules 2001* (Cth) r 2.08.
150 *Family Law Rules 2004* (Cth) r 24.13.
151 *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ss 25, 27, 28, 38G, 38H.

appropriate level; and if the Attorney-General intervenes, the Attorney-General and his or her legal representatives.[152]

Media access to court records

35.105 Media reports are how most members of the public are made aware of court proceedings. Such reports necessarily depend on journalists having access to proceedings, either directly by being permitted to be present at the proceedings, or indirectly by being allowed access to court records. In *Raybos Australia Pty Ltd v Jones*, Kirby P stated that:

> The principles which support and justify the open doors of our courts likewise require that what passes in court should be capable of being reported. The entitlement to report to the public at large what is seen and heard in open court is a corollary of the access to the court of those members of the public who choose to attend … the principles which support open courts apply with special force to the open reporting of criminal trials and, by analogy contempt proceedings … [153]

35.106 Some legislation, however, recognises that certain proceedings may contain particularly sensitive information and should be subject to restricted media reporting. For example, s 121 of the *Family Law Act 1975* (Cth) makes it an offence, except in limited circumstances, to publish proceedings that identify persons or witnesses involved in family law proceedings.[154] Section 91X of the *Migration Act 1958* (Cth) provides that the High Court, the Federal Court and the Federal Magistrates Court must not publish a person's name where the person has applied for a protection visa or a protection-related visa, or had such a visa cancelled.

35.107 One stakeholder submitted that suppression orders, which prohibit the publication of certain information in court proceedings, were a restraint on the media's role of disseminating information to the public. It opposed the granting of suppression orders for the purposes of protecting a person from embarrassment.[155]

Police access to court records

35.108 The Family Law Council submitted that police officers should have access to the Family Court's database so that officers could deal with cases of family violence that arise in the family law context.[156] The ALRC notes that police officers already are allowed to obtain access to the Family Court's database in particular types of matters under the *Family Law Rules 2004* (Cth). Under rule 24.13, with the permission of the

---

152 Ibid ss 29, 38I.

153 *Raybos Australia Pty Ltd v Jones* (1985) 2 NSWLR 47, 55, 58.

154 The restriction does not apply to the publication of accounts of proceedings that have been approved by the court, but the ALRC has been advised that the Family Court has adopted a policy and practice for the anonymisation and pseudonymisation of personal information contained in court records.

155 The Herald and Weekly Times Pty Ltd, *Submission PR 568,* 11 February 2008.

156 Family Law Council, *Submission PR 269,* 28 March 2007.

court, a person is allowed to search, inspect or copy a document forming part of the court record, if he or she can demonstrate a 'proper interest' in the case or the information in the court record.

Party and witness access to court records

35.109 Documents relating to a particular proceeding generally are accessible by parties to the proceeding and their legal representatives.[157] One commentator has asked whether this right should extend to witnesses, on the basis that they are identified in the record and have the right to know what information is held about them.[158]

35.110 Another issue is whether parties should have the right to correct or annotate inaccurate or irrelevant material on the record. It has been argued that, since both freedom of information and privacy legislation gives individuals the right to correct information held about them in public records, the same rule should apply to court records.[159]

35.111 One stakeholder submitted that witnesses should not be able to access court files because 'there is a real risk that the evidence and testimony of that witness may be affected by perusing the court file before giving his or her evidence'. Where access to court records is restricted,

> the information held on the court file, even if inaccurate, is not publicly available and is therefore unlikely to be able to be accessed by or used by someone in a position to adversely affect the witnesses' interests. [160]

35.112 It also was submitted that allowing parties to correct or annotate inaccurate or irrelevant information on the court record 'may contaminate the court record, which is meant to accurately reflect the material before the court rather than commentaries upon the evidence', and would represent a significant 'interference with the role and powers of Courts on appeal where additional evidence may be permitted, but only in limited circumstances'.[161]

35.113 Parties and witnesses to proceedings should not have the right to change or annotate court records. The purpose of court records is to reflect accurately the materials before the court for the purposes of the court's adjudicative functions. The nature of proceedings and the material collected in an adversarial system are inherently contentious. Allowing parties or witnesses to change or annotate court records would

---

157 Some exceptions may apply. For example, in the Federal Court, a party to a proceeding must not search for or inspect specified documents in the court registry without the leave of the court or a judge. These documents include a transcript of the proceeding and a document filed in the proceeding to support an application for an order that a document, evidence or thing be privileged from production: *Federal Court Rules 1979* (Cth) O 46 r 6(5).

158 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 55.

159 Ibid, 55.

160 Confidential, *Submission PR 214*, 27 February 2007.

161 Ibid.

be a significant interference with the court's role as the arbiter of disputes. In addition, court records ought to reflect accurately the materials and evidence on which a court's decision is based, especially for the purposes of review on appeal.

35.114 Allowing witnesses to access court files during proceedings runs the risk that the evidence and testimony of witnesses may be affected before they give evidence. Witnesses are often required to stay out of court in order to avoid the possibility that their testimony changes as a result of what has been seen and heard in court.[162] Similar considerations should apply in relation to court records.

Harmonisation of court and tribunal rules

35.115 In its 2003 strategy paper on the federal civil justice system, the Attorney-General's Department recommended 'that the courts continue to develop, where appropriate, uniform procedures for those areas of law in which the same jurisdiction can be exercised in more than one court'.[163]

35.116 The ALRC reviewed the issue of non-party access to court records as part of its inquiry into the protection of classified and security sensitive information. In ALRC 98, the ALRC identified a number of inconsistencies across state and federal court legislation and rules concerning public access to evidence and other court documents. Inconsistencies included: the types of document that may be accessed; when public access can be presumed; whether leave of the court is required for access; and the release of transcripts to non-parties.[164] The ALRC recommended that SCAG order a review of federal, state and territory legislation and court and tribunal rules relating to non-party access to evidence and other documents produced in relation to proceedings, with a view to developing and promulgating a clear and consistent national policy.[165]

35.117 In recent years, there has been some progress in the harmonisation of court rules in different areas of Australian law. The Council of Chief Justices and the Australian Institute of Judicial Administration have formed a Harmonisation of Rules of Court Committee. The Committee has harmonised rules of court in the areas of corporations law procedure, subpoenas, discovery of documents, and service of process outside the jurisdiction.[166] In 2001, the Federal Court and the Federal Magistrates

---

162 *R v Bassett* [1952] VLR 535; *R v Tait* [1963] VR 520, 523; *Moore v Registrar of Lambeth County Court* [1969] 1 All ER 782, 783; *R v Lister* [1981] 1 NSWLR 110, 114.

163 Australian Government Attorney-General's Department, *Federal Civil Justice System Strategy Paper* (2003), rec 4.

164 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [7.25], [7.36].

165 Ibid, Rec 7–1. This recommendation has not been implemented.

166 Australian Government Attorney-General's Department, *Federal Civil Justice System Strategy Paper* (2003), 67.

Court completed a joint project to develop harmonised rules for bankruptcy proceedings.[167]

35.118 In DP 72, the ALRC observed that there were inconsistencies in legislation and court rules concerning non-party access to court records. For example, some court rules specify, in more detail than others, the categories of documents to which a non-party may have access, with or without leave of the court.[168] There also are differences between court rules as to whether there is a presumption for or against the granting of non-party access to court documents.[169] The ALRC stated that, to the extent that it is appropriate, consistency among rules of courts on non-party access to court documents can enhance clarity and efficiency of the justice system.

Options for reform

35.119 The ALRC considered a number of ways in which non-party access to court records could be standardised. One option is to grant different levels of access for different types of information on court records. In its discussion paper, *Review of the Policy on Access to Court Information*,[170] the Attorney General's Department of New South Wales proposed a system whereby court information is classified as either open to public access or restricted public access.[171] Restricted access information, such as social security and tax file numbers and driver's licence and motor vehicle registration numbers, would be subject to legislative prohibition against media publication.[172] Restricted access information also would be subject to the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW).[173]

35.120 A variation of this first approach is the recommendation in the report on access to court records prepared by the New Zealand Law Commission.[174] The New Zealand Law Commission recommended the enactment of a Court Information Act based on a

---

167 Federal Magistrates Court of Australia, *Annual Report 2005–2006* (2006), 13, 18.

168 Compare, eg, *Court Procedures Rules 2006* (ACT) rr 2903, 4053; *Supreme Court (General Civil Procedure) Rules 2005* (Vic) r 28.05; *Supreme Court (Criminal Procedure) Rules 1998* (Vic) r 1.11.

169 For presumption in favour of non-party access to documents, see, eg, *Rules of the Supreme Court 1971* (WA) O 67 r 11; *Supreme Court Rules 2000* (Tas) r 33; *Court Procedures Rules 2006* (ACT) r 2903. For presumption against access, see, eg, Supreme Court of New South Wales, *Practice Note: Supreme Court—Access to Court Files (No SC Gen 2)* (2006), [5], issued pursuant to s 15 of the *Civil Procedure Act 2005* (NSW).

170 New South Wales Government Attorney General's Department, *Review of the Policy on Access to Court Information* (2006). The options suggested in the paper do not appear to have been considered further or adopted.

171 Ibid, proposal 3.

172 Ibid, proposal 7.

173 Ibid, proposal 10. A prescribed agency may be authorised to obtain specified categories of restricted document provided that the agency is bound by protocols addressing the retention, use and security of the document.

174 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006). The New Zealand Government has referred the report to the Justice and Electoral Select Committee of the New Zealand Parliament for inquiry: New Zealand Government, *Government Response to Law Commission Report on Access to Court Records* (2007).

presumption of open court records limited only by principled reasons for denying access,[175] including the protection of sensitive, private or personal information.[176]

35.121 Another option is to determine the level of access to court records by reference to the nature of the proceedings. In its discussion paper, *Access to Court Records*, the County Court of Victoria proposed that: non-party access to civil files generally be available unless the court orders otherwise; limited access to parties to criminal or appeal files, before and after the trial, at the discretion of the registrar on a case-by-case basis; and no access to criminal or appeal files by non-parties without an order of the court.[177]

35.122 A third option is to remove certain identifying information from the records before publication. In its report on privacy and public access to electronic case files, the United States Committee on Court Administration and Case Management (a committee of the Judicial Conference of the United States) recommended that civil and bankruptcy case files be made available electronically to the same extent they are available at the courthouse, provided that certain 'personal data identifiers' are modified or partially redacted.[178] In September 2003, the Judicial Conference of the United States further permitted remote public access to electronic criminal case files (with certain exceptions) if specified personal identifiers were edited.[179]

35.123 Recently, the Supreme Court of New South Wales issued a policy on the anonymisation of personal information recorded in transcripts and judgments. The stated purpose of the policy was to prevent identity theft and anonymise the identity of accused persons and witnesses where appropriate. The policy requires that certain information be anonymised in judgments and transcripts, such as street numbers, dates of birth, phone numbers, email addresses, tax file numbers and driving licence numbers.[180]

---

175 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), rec R6.

176 Ibid, rec R11.

177 County Court of Victoria, *Discussion Paper: Access to Court Records* (2005), [14], [16], [18], [20]. A new privacy policy outlining the procedures followed by the Court regarding the disclosure of information held in its records was posted on the Court's website and took effect on 1 March 2008: County Court of Victoria, *Privacy* <www.countycourt.vic.gov.au> at 30 April 2008.

178 Social security cases are to be excluded, however, from electronic access: Judicial Conference of the United States—Committee on Court Administration and Case Management, *Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files* <www.privacy.uscourts.gov/Policy.htm> at 1 May 2008.

179 United States Courts, *Judicial Privacy Policy—The Judicial Conference Policy on Privacy and Public Access to Electronic Case Files* <www.privacy.uscourts.gov> at 1 May 2008. The Judicial Conference of the United States approved specific guidance for the implementation of the amended criminal policy in March 2004: United States Courts, *Judicial Privacy Policy—Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files* <www.privacy .uscourts.gov> at 1 May 2008.

180 Supreme Court of New South Wales, *Identity Theft Prevention and Anonymisation Policy* (2007).

35.124 It may be costly for courts to remove identifying information from records before publication. The cost to the courts could be reduced, however, if the person who made the filing was required to file a redacted version of a document for the public record. This option was introduced in the United States by recent amendments to the *Federal Rules of Civil Procedure 2007* (US).[181] Electronic access to court records is discussed further in Chapter 11.

35.125 In DP 72, the ALRC noted submissions by some stakeholders that one set of principles for access to court records would be problematic.[182] One stakeholder submitted that uniform rules on access to court records may fail to take into account the nature and function of specialist courts and tribunals and could have an adverse impact on the interests of persons involved in or affected by litigation.[183] Another stakeholder submitted that the balance between access to, and disclosure of, court records and judgments could not be resolved by one set of principles of general application. It was suggested this was an area where it would be appropriate for the Privacy Commissioner to prepare codes of practice or guidelines.[184]

ALRC's view

35.126 Since federal courts have differing jurisdictions, different considerations apply in relation to the levels of access to their records. For example, the Federal Court and the Federal Magistrates Court have broad jurisdiction, covering a wide range of matters. In contrast, the sensitive nature of the jurisdiction of the Family Court requires specific restrictions on access. It would be inappropriate, therefore, to have one set of access rules for all federal courts. There is, however, merit in promoting consistency in access rules for courts that deal with similar types of cases.

35.127 A coordinated approach by federal, state and territory courts and tribunals to non-party access to court and tribunal records is needed to provide more consistency. The ALRC reaffirms its recommendation in ALRC 98 that SCAG should order a review of federal, state and territory legislation and court and tribunal rules concerning non-party access to court records, with a view to promoting a national and consistent policy.[185]

---

181 *Federal Rules of Civil Procedure 2007* (US) r 5.2.

182 Confidential, *Submission PR 214*, 27 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

183 Confidential, *Submission PR 214*, 27 February 2007.

184 Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

185 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 7–1.

36. Exempt Agencies under the *Freedom of Information Act*

Contents

Introduction

36.1 Currently, a number of agencies that are exempt from the operation of the *Freedom of Information Act 1982* (Cth) (FOI Act) are wholly or partially exempt from the requirements of the *Privacy Act 1988* (Cth).[1] This chapter describes the functions of some of these agencies and considers whether they should remain exempt from the operation of the *Privacy Act*.

1 *Privacy Act 1988* (Cth) ss 7(1)(a)(i)(A)–(C), (b), (c), s 7A.

36.2 It should be noted that all Australian Government agencies, including the agencies discussed in this chapter, are required to comply with the *Protective Security Manual* (PSM 2005).[2] The PSM 2005 is a policy document that sets out guidelines and minimum standards in relation to protective security for agencies and officers, as well as for contractors and their employees who perform services for the Australian Government. In particular, Part C of the PSM 2005 provides 'guidance on the classification system and the protective standards required to protect both electronic- and paper-based security classified information'.[3] It also sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information.

36.3 The PSM 2005 also requires Australian Government agencies to comply with the *Australian Government Information and Communications Technology Security Manual* (ACSI 33). The ACSI 33 has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on the protection of their electronic information systems.[4]

36.4 Although the PSM 2005 addresses some issues that are dealt with under the Information Privacy Principles (IPPs) of the *Privacy Act*, the privacy protection under the PSM 2005 guidelines is restricted to a particular type of information, namely, security classified information. Further, it does not deal with other matters under the IPPs, such as the accuracy of personal information.

Australian Fair Pay Commission

Background

36.5 Section 7(1) of the *Privacy Act* provides that an agency listed in sch 1 of the FOI Act is exempt from the operation of the *Privacy Act*, except in respect of matters of an administrative nature.[5] One of the agencies listed under sch 1 of the FOI Act is the Australian Fair Pay Commission (AFPC). The other agencies listed in sch 1 of the FOI Act are the Australian Industrial Relations Commission (AIRC), and the Industrial Registrar and Deputy Registrars. The exemption of these other agencies is considered in Chapter 35.

36.6 Section 7(1) was originally intended to exempt from the operation of the *Privacy Act* 'industrial tribunals referred to in sch 1 of the FOI Act in respect of administrative matters'.[6] In 2006, the FOI Act was amended to include the AFPC in

---

2 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 8 April 2008.

3 Ibid.

4 Australian Government Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual (ACSI 33)* (2007).

5 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(A), (b).

6 Explanatory Memorandum, Privacy Bill 1988 (Cth), [45].

sch 1 of that Act.[7] The secondary materials relating to the regulations that amended the FOI Act in this way do not disclose the policy behind the exemption of the AFPC from the FOI Act and hence the *Privacy Act*.

36.7 The AFPC is an independent, statutory body established under the *Workplace Relations Amendment (Work Choices) Act 2005* (Cth). The AFPC took over the functions of setting and adjusting federal minimum wages from the AIRC, which retained its role as a national industrial tribunal dealing with employment disputes.[8] The primary functions of the AFPC are to conduct wage reviews and exercise its wage-setting powers as necessary. The main wage-setting powers of the AFPC include adjusting the standard federal minimum wage, as well as determining and adjusting: minimum classification rates of pay; special federal minimum wages for junior employees, employees with disabilities or employees to whom training arrangements apply; basic periodic rates of pay and basic piece rates of pay payable to employees or employees of particular classifications; and casual loadings.[9]

36.8 In exercising its wage-setting powers, the AFPC may inform itself in any way it thinks appropriate, including by: undertaking or commissioning research; consulting with any other person, body or organisation; or monitoring and evaluating the impact of its wage-setting decisions.[10] The AFPC must publish written wage-setting decisions and include reasons in its decisions.[11]

Submissions and consultations

36.9 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC expressed the view that the APFC appeared to be exempt from the *Privacy Act* only by virtue of the fact that it is listed in sch 1 of the FOI Act, and not for any sound policy reasons. The ALRC therefore proposed that the *Privacy Act* be amended to remove the partial exemption that applies to the AFPC under s 7(1) of the Act.[12] There was some support in submissions for the removal of this exemption.[13]

36.10 The Cyberspace Law and Policy Centre supported the proposal on the basis that agencies should not be exempt under the *Privacy Act* simply by virtue of their exempt status under the FOI Act. It argued that any difficulties in compliance with privacy

---

7 *Workplace Relations Amendment (Work Choices) (Consequential Amendments) Regulations (No 1) 2006* (Cth) sch 36.

8 Australian Fair Pay Commission, *About the Commission* <www.fairpay.gov.au/fairpay/About> at 25 March 2008; *Workplace Relations Act 1996* (Cth) s 23.

9 *Workplace Relations Act 1996* (Cth) s 22(1).

10 Ibid ss 24(2).

11 Ibid ss 24(4), 26(1).

12 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 33–1.

13 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

principles should be dealt with by way of selective exceptions to particular principles on the basis of detailed justification.[14] The Public Interest Advocacy Centre also supported the ALRC's proposal, stating that the exemption 'appears to be an anomaly, and has no sound policy justification'.[15]

36.11 In contrast, the Department of Employment and Workplace Relations (DEWR) submitted that the partial exemption that applies to agencies specified under sch 1 of the FOI Act should remain, because agencies that exercise standard-setting, conciliation and quasi-judicial functions should be exempt to the same extent as federal courts. It stated that it was not aware of any compelling arguments to remove the exemption.[16]

36.12 The Office of the Privacy Commissioner (OPC) stated that it has no specific view on whether the AFPC should be exempt from the operation of the *Privacy Act*. It submitted, however, that any decision to maintain the exemption should be justified by 'a clear and demonstrable public interest which reflects community attitudes and values'. The OPC suggested further that consideration should be given to the benefits of treating entities with similar functions consistently under the *Privacy Act.*[17]

36.13 The Office of the Victorian Privacy Commissioner (OVPC) also had no specific view on whether the exemption that applies to the AFPC should be removed, but stated that 'agencies should, as a matter of principle, not be exempted completely'. It submitted that exemptions or exceptions only should apply to specific practices or principles; and that some principles should apply universally, such as the 'Data Security' and 'Data Quality' principles. In addition, the OVPC submitted that 'privacy legislation should only be subject to such reasonable limits … as can be demonstrably justified in a free and democratic society'.[18]

ALRC's view

36.14 The original exemption of agencies that are listed in sch 1 of the FOI Act from the operation of the *Privacy Act* was intended to apply to industrial tribunals, such as the AIRC. Since the AFPC has taken over only the AIRC's wage-setting function and not its dispute resolution function, the original policy justification that applied to industrial tribunals does not apply to the AFPC. Further, there appears to be no stated policy reason for exempting the AFPC from the requirement to comply with the *Privacy Act* in respect of its non-administrative functions. Therefore, it would appear that this exemption of the AFPC from the *Privacy Act* only applies by virtue of the fact that the AFPC is now listed in sch 1 of the FOI Act.

---

14 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
15 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
16 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.
17 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
18 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

36.15 As discussed in Chapter 33, any exemption from the operation of the *Privacy Act* should be limited to the extent possible and justified on sound policy grounds. There does not appear to be any policy justification for the AFPC's exemption. The function of standard setting is not analogous to the exercise of judicial power, which is conferred by the *Australian Constitution*; or to dispute resolution, where there may be an argument that the *Privacy Act* presents barriers to information exchange that is necessary for effective and efficient dispute resolution. The ALRC, therefore, recommends that the exemption that applies to the AFPC be removed.

36.16 In Chapter 35, the ALRC recommends that federal tribunals, commissions and boards whose primary functions involve dispute resolution, administrative review or disciplinary proceedings should be exempt from the operation of the *Privacy Act* except in relation to an act done, or a practice engaged in, in respect of a matter of an administrative nature.[19] Since the AFPC's primary function is wage setting, it does not qualify for the recommended exemption. It may fall under the recommended exemption, however, in the event that the primary function of the AFPC changes to include dispute resolution or administrative review.

36.17 Currently, the AFPC is partially exempt from the provisions of the FOI Act, which does not apply to any request for access to a document of the AFPC unless the document relates to matters of an administrative nature.[20] In Chapter 29, the ALRC recommends that access to personal information held by agencies should continue to be subject to the applicable provisions of any Commonwealth law.[21] Therefore, access to personal information held by the AFPC should remain subject to the FOI Act. The appropriateness of the partial exemption that applies to the AFPC from the operation of the FOI Act could be considered in the ALRC's separate inquiry into the operation of the FOI Act.[22]

Recommendation 36–1 The *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Fair Pay Commission under s 7(1) of the Act.

19 Rec 35–2.
20 *Freedom of Information Act 1982* (Cth) s 6.
21 Rec 29–2.
22 The ALRC has received Terms of Reference to review the FOI Act and related laws to determine whether they continue to provide an effective framework for access to information in Australia.

Schedule 2, Part I, Division 1 of the FOI Act

36.18 Some of the agencies listed in sch 2, Part I, div 1 of the FOI Act—including Aboriginal Land Councils and Land Trusts,[23] the Auditor-General and the National Workplace Relations Consultative Council—are exempt from compliance with the IPPs.[24] They are required, however, to comply with other provisions of the *Privacy Act*, such as the tax file number provisions.[25]

36.19 Section 7A of the *Privacy Act* provides that agencies listed in sch 2, Part I of the FOI Act should be treated as organisations, if prescribed by regulation. Where an agency has been prescribed by regulation for this purpose, it is required to comply with the National Privacy Principles (NPPs) or an approved privacy code. Currently, the only prescribed agencies are the Australian Government Solicitor and the Australian Industry Development Corporation.[26]

Aboriginal Land Councils and Land Trusts

36.20 Aboriginal Land Councils are independent statutory bodies established under the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) to represent Indigenous people in relation to their native title rights. The functions of a Land Council include: ascertaining and expressing the wishes and opinion of Indigenous people living in the area of the Land Council as to the management of, and appropriate legislation concerning, Indigenous land in that area; protecting the interests of traditional Indigenous landowners and other Indigenous people interested in Indigenous land, and consulting with them on any proposal relating to the use of that land; assisting Indigenous people in taking measures to protect sacred sites, carrying out commercial activities on Indigenous land and pursuing traditional land claims; and negotiating with persons having, or desiring to obtain, estates or interests in land which are the subject of a deed of grant held in escrow by a Land Council.[27]

---

23 Aboriginal Land Councils and Land Trusts are created under the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth).

24 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2). The intelligence agencies—namely, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service and the Office of National Assessment—and the Inspector-General of Intelligence and Security also are listed in sch 2, pt I, div 1 of the FOI Act. Issues concerning the exemption of these agencies from compliance with the *Privacy Act* are discussed in Ch 35.

25 Ibid s 7(2). See also Explanatory Memorandum, Privacy Bill 1988 (Cth), [46].

26 *Privacy (Private Sector) Regulations 2001* (Cth) reg 4. Note that the *AIDC Sale Act 1997* (Cth) provides for the sale of AIDC Ltd, the main operating subsidiary of the Australian Industry Development Corporation, and the progressive winding-down of the Australian Industry Development Corporation. AIDC Ltd was sold in 1998: Commonwealth of Australia, *Commonwealth National Competition Policy—Annual Report 1997–98* (1999). Due to some long term obligations, however, the winding down of the Australian Industry Development Corporation is unlikely to be completed before 2010: Australian Industry Development Corporation, *Statement of Intent* <www.finance.gov.au/gbab/docs/AIDC_SOI.pdf> at 14 May 2008.

27 *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23.

36.21 Aboriginal Land Trusts were established under the *Aboriginal Land Rights (Northern Territory) Act* to hold title to land in the Northern Territory for the benefit of Indigenous people entitled by Indigenous tradition to the use or occupation of the land.[28] Land Trusts are responsible for: holding the title to land vested in it in accordance with the *Aboriginal Land Rights (Northern Territory) Act*; exercising its powers as owner of land for the benefit of the Indigenous people concerned; and where a Land Trust is named as the grantee of land in a deed of grant held in escrow by a Land Council, acquiring the estates and interests of other persons in the land with a view to surrendering those estates and interests to the Crown and delivering the deed of grant held by the Land Council to the Land Trust.[29]

36.22 Aboriginal Land Councils and Land Trusts are exempt from the requirement to comply with the provisions of the FOI Act because they are separate from the executive arm of the government and therefore are not subject to public sector responsibilities.[30] While not stated expressly in any secondary materials, it is likely that this also is the reason that these bodies were exempted from the *Privacy Act* when that Act applied only to the public sector. It is unclear why they remain exempt from the *Privacy Act* now that the Act has been extended to the private sector.

Auditor-General

36.23 The Auditor-General is an independent statutory officer responsible for auditing the activities of most Commonwealth public sector entities. The Auditor-General is supported by the Australian National Audit Office, which provides the Australian Parliament with an independent assessment of certain areas of public administration, and assurance about public sector financial reporting, administration and accountability. The Auditor-General has broad information-gathering powers and the authority to access Commonwealth premises.[31] While the Auditor-General is not required to comply with the IPPs, s 36(1) of the *Auditor-General Act 1997* (Cth) provides that a person who has obtained information in the course of performing an Auditor-General function must not disclose that information except in the course of performing that function.

National Workplace Relations Consultative Council

36.24 The National Workplace Relations Consultative Council is a consultative body that provides a forum for representatives of the Australian Government, employers and employees to discuss workplace relations matters of national concern.[32] In its review of

28 Ibid s 4.
29 Ibid s 5.
30 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].
31 *Auditor-General Act 1997* (Cth) pt 5 div 1.
32 *National Workplace Relations Consultative Council Act 2002* (Cth) s 5.

the Freedom of Information Bill 1978 (Cth), the Senate Standing Committee on Constitutional and Legal Affairs expressed the view that the Council should not be exempt from the FOI legislation because it was a consultative body rather than a conciliatory body, and the Council's proceedings would be protected from disclosure adequately under another provision of the Bill that exempts internal consultative or deliberative documents from the operation of the Bill.[33]

36.25 During parliamentary debate on the Freedom of Information Bill 1981 (Cth), a number of parliamentarians commented that there was no reasonable justification for exempting many of the agencies in sch 2 of the Bill, many of which did not have commercial or intelligence functions.[34] Particular mention was made of the Aboriginal Land Councils and Land Trusts, the Auditor-General and the former National Labour Consultative Council (now the National Workplace Relations Consultative Council).[35]

36.26 In their 1994 inquiry into the FOI Act, the ALRC and the Administrative Review Council (ARC) commented that decisions to exempt particular agencies from the FOI Act have tended to be selective.[36] The ALRC and ARC recommended that all agencies listed in sch 2, Part I of the FOI Act (other than the intelligence agencies, the Inspector-General of Intelligence and Security and government business enterprises) should be required to demonstrate to the Attorney-General the grounds on which they should be exempt from the operation of that Act. If they did not do this within 12 months, the ALRC and the ARC recommended that they should be removed from sch 2, Part I of that Act.[37]

36.27 On 5 September 2000, the Freedom of Information Amendment (Open Government) Bill 2000 (Cth) was introduced as a Private Member's Bill into the Senate by Senator Andrew Murray. The Bill was designed to amend the FOI Act to

---

33 Parliament of Australia—Senate Standing Committee on Constitutional and Legal Affairs, *Freedom of Information—Report by the Senate Standing Committee on Constitutional and Legal Affairs on the Freedom of Information Bill 1978, and Aspects of the Archives Bill 1978* (1979), [12.36].

34 Commonwealth, *Parliamentary Debates*, House of Representatives, 18 August 1981, 44 (L Bowen), 47–48; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 August 1981, 49 (I Harris), 50–51; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 428 (B Jones), 430–431; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 439 (D Cameron), 439–440; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 440 (P Milton), 441; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 379 (A Theophanous), 381; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 388 (J Carlton), 389–390; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 391 (B Howe), 393.

35 Commonwealth, *Parliamentary Debates*, House of Representatives, 18 August 1981, 49 (I Harris), 51; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 439 (D Cameron), 439–440; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 440 (P Milton), 441; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 379 (A Theophanous), 381; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 391 (B Howe), 393.

36 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

37 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 74.

give effect to recommendations made by the ALRC and the ARC. One proposal under the Bill was to revoke the exempt status of many of the agencies, and of particular documents of certain agencies, listed in sch 2 of the FOI Act.[38]

36.28 The provisions of the Bill were referred to the Senate Legal and Constitutional Legislation Committee for inquiry. In its report, the Committee did not support the proposal to revoke the exempt status of these agencies and documents. It was of the view that alternative ways of structuring the exemption provisions under the FOI Act should be examined more closely before amending the legislation.[39] The Bill was amended to remove the proposal.[40]

Schedule 2, Part II, Division 1 of the FOI Act

36.29 A number of agencies listed in sch 2, Part II, Division 1 of the FOI Act are exempt from the *Privacy Act* where their acts and practices relate to documents specified in the FOI Act, to the extent that those documents relate to the non-commercial activities of the agencies or of other entities.[41] In relation to documents that are *not* specified under the FOI Act, these agencies are covered by the IPPs where the documents concern the agencies' non-commercial activities or the non-commercial activities of other entities.[42] These agencies also are covered by the NPPs where their acts and practices relate to commercial activities or to documents concerning commercial activities.[43] In addition, they are required to comply with the tax file number provisions and, where applicable, the credit reporting provisions of the *Privacy Act*.[44] These agencies are described below.

Financial departments and agencies

36.30 The Department of the Treasury focuses primarily on economic policy and has four principal functions: (i) fostering a sound macroeconomic environment; (ii) providing advice to government on effective government spending and taxation arrangements; (iii) assisting in the formulation and implementation of effective taxation and retirement income arrangements; and (iv) providing advice to government on policy processes and reforms that promote markets that function effectively.[45] The Department's acts and practices relating to documents concerning the activities of the

38 See Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [1.1]–[1.2], [3.31].
39 Ibid, [3.137].
40 The Bill was lapsed with the prorogue of successive Australian Parliaments, but has been restored to the notice papers a number of times and is currently before the Senate as the Freedom of Information (Open Government) Bill 2003 [2008].
41 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.
42 Ibid s 7(1)(c).
43 Ibid s 7A.
44 Ibid s 7(2).
45 Australian Government—The Treasury, *About Treasury* <www.treasury.gov.au> at 25 March 2008.

Australian Loan Council are exempt from the IPPs and NPPs, to the extent that those documents relate to non-commercial activities.[46] The Australian Loan Council is a Commonwealth-State ministerial council that coordinates public sector borrowing. The Prime Minister and the premier or chief minister of each state and territory constitute the Council.[47]

36.31 The Reserve Bank of Australia is a statutory authority that is responsible for: formulating and implementing monetary and banking policy; maintaining financial system stability; contributing to the maintenance of full employment in Australia; and promoting the safety and efficiency of the payments system. It actively participates in financial markets, manages Australia's foreign reserves, issues Australian currency notes and serves as banker to the Australian Government.[48] The Reserve Bank has the power to: receive money on deposit; borrow and lend money; buy, sell, discount and re-discount bills of exchange, promissory notes and treasury bills; buy and sell securities issued by the Australian Government and other securities; buy, sell and otherwise deal in foreign currency, specie, gold and other precious metals; establish credits and give guarantees; issue bills and drafts and effect transfers of money; underwrite loans; and issue, re-issue or cancel Australian notes.[49] The Reserve Bank is exempt from compliance with the *Privacy Act* where its acts and practices relate to documents concerning its banking operations (including individual open market operations and foreign exchange dealings) or exchange control matters, to the extent that these documents relate to non-commercial activities.[50]

36.32 The Export Finance and Insurance Corporation is a self-funded statutory corporation wholly owned by the Australian Government. It provides specialist financial and insurance services to Australian companies exporting and investing overseas.[51] The Corporation is exempt from the operation of the *Privacy Act* where its acts and practices relate to documents concerning anything it has done under Part 4 (insurance and financial services and products) or Part 5 (national interest transactions) of the *Export Finance and Insurance Corporation Act 1991* (Cth), to the extent that those documents relate to non-commercial activities.[52]

Australian Transaction Reports and Analysis Centre

36.33 The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit. It is located within the portfolio of the Attorney-

---

46 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

47 Australian Government, *2007–08 Budget Paper No 3—Federal Financial Relations 2007–08* (2007), 35.

48 Reserve Bank of Australia, *About the RBA* <www.rba.gov.au/AboutTheRBA/> at 25 March 2008. See also *Reserve Bank Act 1959* (Cth) s 10.

49 *Reserve Bank Act 1959* (Cth) ss 8, 34.

50 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

51 Australian Government Export Finance Insurance Corporation, *About Us* <www.efic.gov.au> at 25 March 2008.

52 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

General. AUSTRAC oversees compliance with the reporting requirements of the *Financial Transaction Reports Act 1988* (Cth) and the *Anti-Money Laundering and Counter-terrorism Financing Act 2006* (Cth) (AML/CTF Act) by financial services providers, the gambling industry and others. It also provides financial transaction report information to federal, state and territory law enforcement, security, social justice and revenue agencies, as well as to certain international counterparts.[53] AUSTRAC is exempt from compliance with the *Privacy Act* in respect of documents concerning certain information, namely:

- reports of suspected illegal transactions by cash dealers involving currency in excess of $10,000 under s 16 of the *Financial Transaction Reports Act*; [54]

- reports of suspicious matters—that is, matters where there are reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorism financing or money laundering—under s 41 of the AML/CTF Act; and

- information requested by AUSTRAC from a reporting entity[55] in relation to reports of suspicious matters, threshold transactions[56] and certain international funds transfer transactions under s 49 of the AML/CTF Act.[57]

36.34 Part 11 of the AML/CTF Act contains secrecy and access provisions concerning information obtained or held by AUSTRAC. Section 123 of the AML/CTF Act creates an offence of 'tipping off'. A reporting entity is prohibited from disclosing that it has: formed a suspicion about a transaction or matter; given, or is required to give, a suspicious matter report to AUSTRAC; or provided further information under s 49(1) of the AML/CTF Act.[58] A similar provision in the *Financial Transaction Reports Act* applies to cash dealers in relation to suspected illegal transactions.[59]

---

53 AUSTRAC, *About AUSTRAC* <www.austrac.gov.au> at 25 March 2008.

54 A 'cash dealer' is defined to include, for example, a financial institution, an insurer or an insurance intermediary, a person who carries on a business of collecting, holding, exchanging, remitting or transferring currency on behalf of other persons: *Financial Transaction Reports Act 1988* (Cth) s 3.

55 A reporting entity is a person who provides a 'designated service': *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5. Designated services include a wide range of specified financial services, bullion trading services, gambling services and other prescribed services: *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 6.

56 A 'threshold transaction' means a transaction involving the transfer of not less than $10,000 of physical currency or e-currency, or a transaction specified in regulations to be a threshold transaction: *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5.

57 *Privacy Act 1988* (Cth) s 7(1)(c).

58 This is subject to certain exceptions under s 123(4)–(8) of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

59 *Financial Transaction Reports Act 1988* (Cth) s 16(5A), (5AA).

36.35 An AUSTRAC official is prohibited from disclosing information or documents collected, compiled or analysed by AUSTRAC except for the purposes of: the AML/CTL Act or the *Financial Transaction Reports Act*; the performance of the functions of the Chief Executive Officer of AUSTRAC (AUSTRAC CEO); or the performance of the official's duties under the AML/CTL Act or the *Financial Transaction Reports Act*.[60] In addition, AUSTRAC officials and other investigating officials (such as the Commissioner of the Australian Federal Police and the Chief Executive Officer of the Australian Crime Commission) are prohibited from disclosing any information obtained under s 49 of the AML/CTL Act except for the purposes of the AML/CTL Act or the *Financial Transaction Reports Act*, or in connection with their official functions and duties.[61]

36.36 In the performance of his or her functions, the AUSTRAC CEO must consult with, and consider the views of, a number of entities and agencies, including the Privacy Commissioner.[62]

36.37 The interaction between the AML/CTF Act and the *Privacy Act* is discussed further in Chapter 16.

Media regulatory agencies

36.38 The Australian Communications and Media Authority (ACMA) is a statutory body responsible for the regulation of broadcasting, radiocommunications, telecommunications and the internet. Its responsibilities include: promoting self-regulation and competition in the telecommunications industry, while protecting consumers and other users; fostering an environment in which electronic media respects community standards and responds to audience and user needs; managing access to the radiofrequency spectrum; and representing Australia's communications and broadcasting interests internationally.[63]

36.39 The Classification Board and the Classification Review Board are separate and independent statutory bodies. The Classification Board classifies films (including videos and DVDs), computer games and certain publications before they are made available to the public. It also provides classifications to ACMA on internet content, advice to enforcement agencies such as the police, and advice to the Australian Customs Service.[64] The Classification Review Board is a part-time body that reviews

---

60 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 121.

61 Ibid s 122.

62 The AUSTRAC CEO also must consult with reporting entities or their representatives, and the heads of specified investigative agencies: Ibid s 212(2).

63 *Australian Communications and Media Authority Act 2005* (Cth) pt 2 div 2; Australian Communications and Media Authority, *Client Service Charter* <www.acma.gov.au> at 25 March 2008.

64 Australian Government, *The Classification Board* <www.classification.gov.au> at 25 March 2008.

the classification of films, publications or computer games upon receipt of a valid application to review the decisions of the Classification Board.[65]

36.40 The Office of Film and Literature Classification was an agency within the Attorney-General's portfolio that provided support to the Classification Board and the Classification Review Board. On 1 July 2007, the Attorney-General's Department (AGD) took over the policy and administrative functions of the Office of Film and Literature Classification and the Office ceased to exist as a separate agency.[66]

36.41 ACMA, the Classification Board, the Classification Review Board and the AGD are exempt from the *Privacy Act* where their acts and practices concern 'exempt content-service documents' or 'exempt Internet-content documents' under schs 5 and 7 to the *Broadcasting Services Act 1992* (Cth).[67] An 'exempt content-service document' means a document containing offensive content that has been delivered or accessed using a content service; or a document that sets out how to access, or is likely to facilitate access to, offensive content-service content.[68] An 'exempt Internet-content document' is a document containing offensive information that has been copied from the internet; or a document that sets out how to access, or is likely to facilitate access to, offensive information on the internet.[69]

National broadcasters

36.42 The Australian Broadcasting Corporation (ABC) is a statutory corporation and Australia's only national, non-commercial broadcaster. The Special Broadcasting Service (SBS) is Australia's multicultural and multilingual public broadcaster. The SBS was established under the *Special Broadcasting Service Act 1991* (Cth) to provide multilingual and multicultural radio and television services.[70]

---

65 Australian Government, *The Classification Review Board* <www.classification.gov.au> at 25 March 2008.

66 Australian Government Attorney-General's Department, *Administrative Arrangements for the Classification Board and Classification Review Board* <www.ag.gov.au/www/agd/agd.nsf/Page/RWPEB9317B18576C244CA2572D700023C62> at 6 August 2007.

67 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

68 *Freedom of Information Act 1982* (Cth) s 4(1). Subject to a number of exceptions, a 'content service' means a service that delivers content by means of a carriage service to persons having equipment appropriate for receiving that content, or a service that allows end-users to access content using a carriage service: *Broadcasting Services Act 1992* (Cth) sch 7 cl 2. 'Carriage service' means a service for carrying communications by means of guided or unguided electromagnetic energy: *Broadcasting Services Act 1992* (Cth) sch 7 cl 2; *Telecommunications Act 1997* (Cth) s 7.

69 *Freedom of Information Act 1982* (Cth) s 4(1).

70 *Special Broadcasting Service Act 1991* (Cth) s 6.

36.43 Pursuant to s 7(1)(c) of the *Privacy Act*, both the ABC and the SBS are covered by the *Privacy Act* except in relation to their program materials[71] and datacasting content.[72] Section 7A of the Act provides, however, that despite s 7(1)(c), certain acts and practices of the agencies listed in sch 2, Part II, div 1 of the FOI Act (including the ABC and the SBS) are to be treated as acts and practices of organisations. These include acts and practices in relation to documents concerning their commercial activities or the commercial activities of another entity, and acts and practices that relate to those commercial activities.[73] Therefore, it would appear that, apart from their program materials and datacasting content, the ABC and the SBS are covered by the IPPs in relation to non-commercial activities, and the NPPs in relation to commercial activities. To the extent that their program materials and datacasting content relate to commercial activities, they are covered by the private sector provisions of the *Privacy Act*.

36.44 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) stated, however, that s 7A was not intended to apply to the ABC and the SBS.

> The effect of new clause 7A is to make the acts and practices of some agencies subject to the standards in the NPPs (or an approved privacy code, as appropriate), to the extent that they are not currently subject to the Information Privacy Principles (by virtue of section 7 of the Act). The Government's policy is that bodies operating in the commercial sphere should operate on a level playing field. Where agencies are engaged in commercial activities, they should be required to comply with the NPPs, just like private sector organisations …
>
> The aim of the amendment is to ensure that an agency in Division 1 of Part II of Schedule 2 to the FOI Act complies with the standards set out in the NPPs or an approved privacy code (as appropriate) in relation to documents in respect of its commercial activities or the commercial activities of another entity. This clause is intended to apply to agencies such as Comcare, the Health Insurance Commission and

---

71 In *Rivera v Australian Broadcasting Corporation* (2005) 222 ALR 189, Hill J of the Federal Court of Australia held that s 7(1)(c) of the *Privacy Act* operated so as to exempt any acts and practices of the ABC dealing with records concerning its program material and therefore the court had no jurisdiction to grant relief under the Act. One commentator observed that the court's attention had not been drawn to all the relevant provisions of the Act, including the journalism exemption and s 7A which provides that *despite* s 7(1)(c), the ABC is subject to the NPPs where its acts and practices concerns commercial activities: P Gunning, 'Cases + Complaints: Rivera v Australian Broadcasting Corporation [2005] FCA 661' (2004) 11 *Privacy Law & Policy Reporter* 205. In *Australian Broadcasting Corporation v The University of Technology, Sydney* (2006) 91 ALD 514, Bennett J of the Federal Court of Australia held that the ABC is exempt under the *Freedom of Information Act 1982* (Cth) in relation to documents that have a direct or indirect relationship to ABC's program materials, provided that those documents also have a relationship to the ABC.

72 'Datacast' means to broadcast digital information: *Macquarie Dictionary* (online ed, 2007). Under s 6 of the *Broadcasting Services Act 1992* (Cth), 'datacasting service' means a service that delivers content using the broadcasting services bands—whether in the form of text; data; speech, music or other sounds; visual images; or any other form—to persons with the appropriate equipment for receiving that content.

73 *Privacy Act 1988* (Cth) s 7A.

> Telstra Corporation Limited. It is not intended to apply to the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.[74]

36.45 Where the acts and practices of the ABC and the SBS are to be treated as those of organisations, they may still be exempt if carried out in the course of journalism.[75] The exemption relating to journalism is discussed in Chapter 42.

Austrade

36.46 The Australian Trade Commission (Austrade) was established by the *Australian Trade Commission Act 1985* (Cth). Its functions are to provide advice, market intelligence and support to Australian companies to reduce the time, cost and risk involved in selecting, entering and developing international markets. In addition, it provides advice and guidance on overseas investment and joint venture opportunities. Austrade also administers the Export Market Development Grants scheme, which provides financial assistance to eligible businesses through partial reimbursement of the costs of specified export promotion activities.[76]

36.47 Austrade is exempt from the operation of the *Privacy Act* where its acts and practices relate to documents concerning the carrying out of overseas development projects, to the extent that these documents relate to non-commercial activities.[77]

National Health and Medical Research Council

36.48 The National Health and Medical Research Council (NHMRC) is a statutory agency responsible for promoting the development and maintenance of public and individual health standards. It does this by fostering the development of consistent health standards between states and territories, fostering health and medical research and training, and monitoring ethical issues relating to health throughout Australia.[78]

36.49 The NHMRC is exempt from the *Privacy Act* where its acts and practices relate to documents in the possession of its Council members who are not persons appointed or engaged under the *Public Service Act 1999* (Cth), to the extent that these documents relate to non-commercial activities.[79]

---

74 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [102], [104].

75 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(4).

76 *Australian Trade Commission Act 1985* (Cth) ss 7A, 8; Austrade, *What is Austrade?* <www.austrade.gov.au> at 25 March 2008.

77 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A. An 'overseas development project' is a project to be carried out in a foreign country by way of: the construction of works; the provision of services; the design, supply or installation of equipment or facilities; or the testing in the field of agricultural practices: *Australian Trade Commission Act 1985* (Cth) s 3(1).

78 National Health and Medical Research Council, *Role of the NHMRC* <www.nhmrc.gov.au/about/role/index.htm> at 25 March 2008. See also *National Health and Medical Research Council Act 1992* (Cth) ss 5C, 7.

79 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

Submissions and consultations

36.50 In DP 72, the ALRC observed that the exemption of agencies listed under sch 2 of the FOI Act from the *Privacy Act* appeared to derive from their exempt status under the FOI Act. The ALRC noted that it had not received submissions from most of the relevant agencies and, accordingly, could not make an informed policy decision about whether they should remain exempt from compliance with the *Privacy Act*. The ALRC considered, however, that the relevant agencies should be provided with a final opportunity to make a case for retaining their exempt status if they considered their exemption from the *Privacy Act* justified.

36.51 The ALRC proposed, therefore, that certain agencies listed in Part I, div 1 and Part II, div 1 of sch 2 of the FOI Act be required to demonstrate to the Attorney-General that they warrant exemption from the operation of the *Privacy Act*. Those agencies included the Aboriginal Land Councils and Land Trusts, the Auditor-General and the National Workplace Relations Consultative Council, the Department of the Treasury, the Reserve Bank of Australia, the Export and Finance Insurance Corporation, ACMA, the Classification Board, the Classification Review Board, Austrade and the NHMRC. The ALRC further proposed that the exemption be removed if the relevant agency did not make an adequate case for retaining its exempt status.[80]

36.52 A number of stakeholders supported this proposal.[81] The OPC stated that exemptions should be kept to a minimum and justified on the basis of clear policy or public interest. Further, it submitted that any exemptions from the operation of the *Privacy Act* should be defined clearly. The OPC also suggested that a review of the existing exemptions from the *Privacy Act* should address irregularities in the coverage of the exemptions, and the potential of the exemptions to undermine national consistency and promote fragmentation in privacy regulation. While the OPC was not aware of any 'clear and compelling justifications' for the exemption of the agencies discussed in this chapter, it supported the approach proposed by the ALRC to determine the appropriateness of their exempt status.[82]

36.53 Some stakeholders expressed the view that agencies should not be exempt automatically from the operation of the *Privacy Act* by virtue of their exempt status under the FOI Act,[83] particularly given the different policy objectives of the *Privacy*

---

80 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 33–2.

81 See, eg, 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; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

83 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

Act and the FOI Act.[84] The Cyberspace Law and Policy Centre submitted that any difficulties in complying with privacy principles should be dealt with by way of selective exceptions to particular principles on the basis of detailed justification. It further suggested that these agencies also should justify their exemption from related provisions of the FOI Act.[85]

36.54 Other stakeholders also supported the proposal, but submitted that any review of the exemption of the agencies discussed in this chapter from the operation of the *Privacy Act* should be subject to a process of public consultation and allow for other interested parties, such as privacy advocates and consumer groups, to make submissions on the issue.[86]

36.55 The OVPC submitted that agencies should not be exempt completely from the *Privacy Act*. It was of the view that exemptions or exceptions should apply only to specific practices or principles, and that certain principles should apply universally, such as the 'Data Security' and 'Data Quality' principles. In addition, it suggested that 'privacy legislation should only be subject to such reasonable limits … as can be demonstrably justified in a free and democratic society'.[87]

Aboriginal Land Councils and Land Trusts

36.56 One stakeholder specifically supported the removal of the exemption that applies to Aboriginal Land Councils and Land Trusts. It submitted, however, that the exemption should be removed as soon as possible, noting that certain land councils and land trusts have 'repeatedly ignored or otherwise refused' requests by Aboriginal people for access to their personal information, including information about their traditional rights and interests in lands and seas.[88]

36.57 The Law Council of Australia noted that the need for specialised consultations with Indigenous organisations had been identified in other legal contexts, such as native title and heritage protection. It therefore suggested that the appointment of an Indigenous consultant for the purpose of specific consultation with Indigenous organisations on the exemption would be desirable.[89]

NHMRC

36.58 The NHMRC advised that it is 'unaware of the reasons for the exemption in the *Freedom of Information Act* and would not object to the exemption [under the *Privacy*

---

84 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
85 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
86 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
87 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
88 Midena Lawyers, *Submission PR 363*, 3 December 2007.
89 Law Council of Australia, *Submission PR 527*, 21 December 2007.

Act] being removed'. It observed, however, that the exemption of the NHMRC from the FOI Act also may be reviewed in the context of the ALRC's current inquiry into the FOI Act.[90]

AUSTRAC

36.59 In DP 72, the ALRC expressed the view that the exemption that currently applies to AUSTRAC should remain. The ALRC noted that the exemption is limited to AUSTRAC's law enforcement functions, and expressed the view that the application of the Unified Privacy Principles (UPPs) to AUSTRAC could cause difficulties for AUSTRAC's operations. Further, the ALRC noted that AUSTRAC officials are subject to strong information-handling and secrecy provisions.[91]

36.60 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre submitted that, like other agencies that are exempt from both the FOI Act and the *Privacy Act*, AUSTRAC also should have to justify its exemption from the *Privacy Act*.[92]

36.61 AUSTRAC submitted that its partial exemption from the *Privacy Act* should remain. It suggested that there are two important policy reasons behind the exemption concerning the reporting of suspected illegal transactions. First, individuals should not be alerted to the fact that suspect transaction reports were made in relation to them because

> such reports may be relevant to criminal investigations or investigation relating to terrorism financing and tipping off may prejudice those investigations. In addition, cash dealer staff members that report such transactions may be put at risk if it is disclosed that a suspect transaction report has been lodged.[93]

36.62 AUSTRAC stated that cash dealers have legitimate concerns about protecting their staff from retribution for filing a suspected transaction report. It submitted that if information concerning the existence of a suspected transaction report could become known to the subject of the report, there would be a decrease in both the number and quality of suspected transaction reports.[94]

36.63 AUSTRAC submitted further that 'protecting the privacy of AUSTRAC's information is a key priority for the agency'. It submitted that there is a high level of privacy protection in relation to AUSTRAC's information. In particular, information held by AUSTRAC is protected by:

---

90 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

91 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [33.62]—[33.63].

92 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

93 AUSTRAC, *Submission PR 216*, 1 March 2007.

94 Ibid.

- the provision of training for all staff on privacy requirements;
- secrecy and access provisions under Part 11 of the AML/CTF Act;
- limited access to AUSTRAC information pursuant to an Instrument of Authorisation signed by the AUSTRAC CEO under s 126(1) of the AML/CTF Act;
- Memoranda of Understanding between the AUSTRAC CEO and the Chief Executive of 29 of the 33 designated agencies that are entitled or authorised to have access to AUSTRAC information;
- audit trails of access to suspected transactions reports by its own staff, the Australian Taxation Office and designated agency officers; and
- a legislative requirement that, in the performance of his or her functions, the AUSTRAC CEO consult with the Privacy Commissioner.[95]

ABC and SBS

36.64 In DP 72, the ALRC expressed the view that the exemption of the ABC and the SBS from the *Privacy Act* by virtue of their exempt status under the FOI Act was not justified, and that they should not be treated differently from media organisations in the private sector. The ALRC therefore proposed that the exemption that applies to the ABC and the SBS under the *Privacy Act* be removed.[96]

36.65 Some stakeholders supported this proposal.[97] The OPC did not comment specifically on whether the exemption that applies to the ABC and the SBS should remain. It stated, however, that it supported the retention of the journalism exemption in its revised form, which would apply to exempt the ABC and the SBS from the *Privacy Act* in the context of their journalistic activities.[98]

36.66 Both the ABC and the SBS submitted that their exemption from the *Privacy Act* should be retained, on the basis that their programming materials are not 'commercial activities' and therefore are not, and should not be, subject to the *Privacy Act*. They argued that they should not be regarded as being in commercial competition with

---

95 Ibid.

96 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 33–3.

97 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

98 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. The journalism exemption is discussed in detail in Ch 42.

private sector media organisations because they have specific statutory functions and governance requirements that are different from those that apply to other media organisations.[99] The ABC and the SBS submitted further that being exempt from the operation of the IPPs and NPPs in relation to their program-making activities does not mean that they are not subject to privacy regulation or oversight. They observed that they are subject to privacy provisions in their editorial policies, as well as codes of practice that are lodged with ACMA, which investigates complaints about alleged breaches of the codes.[100]

36.67 The SBS submitted that removing the exemption 'would affect the ability of national broadcasters to carry out their unique role in the Australian media, cultural and political landscape'. It observed that both the ABC and the SBS have statutory functions to inform, educate and entertain Australians, and that they play an important role in communicating political, cultural and other information to the Australian public. The SBS argued that the importance of its role is recognised by its enabling legislation, which establishes certain standards for programming as well as a duty to maintain the independence of the SBS.[101]

36.68 The SBS also submitted that it should continue to be exempt in relation to access to, and correction of, personal information. The SBS was concerned that allowing access to, and correction of, personal information in relation to its program materials would have implications for matters such as the protection of copyright and confidentiality of sources; and may impede the free flow of information to the public, for example, if an injunction were granted based on knowledge of the program's content. The SBS observed that, while a number of these situations would be covered by other exemption provisions in the FOI Act, such as the exemption for internal working documents and documents relating to business affairs, they lack the certainty an exemption for the SBS's program materials provides. In addition, the SBS argued that the need to consider requests for access on a case-by-case basis 'could impede the timeliness and topicality of its news and current affairs reporting and have a deleterious effect on its independence and integrity'.[102]

36.69 Further, the SBS argued that removing the exemption of the SBS and the ABC from the operation of provisions dealing with access to, and correction of, personal information in either the FOI Act or the *Privacy Act* would subject the national broadcasters to an additional layer of regulation and accountability that does not apply to other broadcasters.[103]

---

99 Australian Broadcasting Corporation, *Submission PR 571,* 18 February 2008; Special Broadcasting Service, *Submission PR 530,* 21 December 2007.

100 Special Broadcasting Service, *Submission PR 530,* 21 December 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

101 Special Broadcasting Service, *Submission PR 530,* 21 December 2007.

102 Ibid.

103 Ibid.

36.70 The ABC was concerned that, in the event that its exemption from the *Privacy Act* is removed, its journalistic activities would not fall under the journalism exemption and therefore would be subject to the IPPs. The ABC argued that, since its program materials do not relate to 'commercial activities', s 7A of the *Privacy Act*—which requires that certain agencies comply with the NPPs in relation to their commercial activities—would not apply to deem the ABC to be an 'organisation' and therefore it would not be a 'media organisation' for the purposes of the journalism exemption.[104]

36.71 In addition, the ABC argued that the fact that the ABC and the SBS Boards oversee the development of the national broadcasters' codes of practice, without the need for prior consultation with ACMA, clearly indicates that Parliament has recognised the primary role of the Boards in overseeing programming-related matters. The ABC submitted that the proposed removal of its exemption would reduce the ABC Board's statutory oversight of the ABC's program activities by empowering the Privacy Commissioner to deal with privacy-related complaints in relation to such activities and interfere with the role of ACMA in investigating alleged breaches of the privacy provisions of the ABC's Code of Practice. It argued that:

> the role envisaged for the Privacy Commissioner that will follow from removal of the … exemption runs directly counter to that governance regime, and would constitute a significant encroachment on the ABC's statutory independence.[105]

ALRC's view

36.72 The exemption of the agencies listed under sch 2 of the FOI Act from the *Privacy Act* is expressed in terms of their exemption from the FOI Act. Therefore, their exemption from the operation of the *Privacy Act* derives from their status under the FOI Act. The purposes of the *Privacy Act* are, however, different from those of the FOI Act. The *Privacy Act* is mainly concerned with the protection of the privacy of personal information about individuals, whereas the FOI Act aims to promote the ideals of an open and transparent government by granting a right of access to, and correction of, government records, except in relation to certain exempt documents. Given the differing purposes of the two Acts, it is inappropriate to exempt agencies from compliance with the *Privacy Act* simply because they are exempt from the operation of the FOI Act. There should be clear policy justifications for the exemption of these agencies from the *Privacy Act*.

104 Australian Broadcasting Corporation, *Submission PR 571*, 18 February 2008.
105 Ibid.

36.73 The ALRC has not received submissions from a number of the exempt agencies about their exemption from the operation of the *Privacy Act*, despite specifically inviting submissions from them.[106] In these circumstances, the ALRC is unable to make an informed policy decision about whether these agencies should remain exempt from the operation of the *Privacy Act*. The ALRC notes that some overseas jurisdictions, such as the United Kingdom and Hong Kong, exempt very few specified agencies from the operation of their privacy legislation.[107] Exemptions in these overseas jurisdictions are based on the activities of particular types of data controllers, rather than for specified, named data controllers. It is difficult, therefore, to compare the agencies discussed in this chapter with overseas agencies that are exempt from their privacy legislation.

36.74 Certain agencies discussed in this chapter should be required to demonstrate to the minister responsible for administering the *Privacy Act* that they warrant exemption from compliance with the *Privacy Act*. In the event that these agencies fail to do so within 12 months, their exempt status should be revoked automatically. This approach would give the relevant agencies a final opportunity to consider their position and make their case if they believe an exemption is warranted. The ALRC notes that this option also was generally supported in submissions.

36.75 The ALRC also notes submissions by some stakeholders that interested parties, such as privacy advocates, should be able to make submissions on the issue of whether the agencies discussed in this chapter should be exempt from the operation of the *Privacy Act*. The ALRC agrees that as a matter of informed and transparent policy making, there should be public consultation on any claims for exemption, as well as consultations with the OPC and other interested stakeholders. In the case of Aboriginal Land Trusts and Land Councils, consultation, particularly with Indigenous representative groups, would be appropriate.

NHMRC

36.76 In DP 72, the ALRC proposed that the NHMRC be included in the list of agencies that are required to demonstrate that they warrant exemption from the operation of the *Privacy Act*. The NHMRC has since submitted that it was unaware of the reasons for its partial exemption from the operation of that Act and would not object to the exemption being removed. The ALRC therefore recommends that the partial exemption that applies to the NHMRC under the *Privacy Act* be removed.

---

106 In October 2006, the ALRC wrote to the following agencies inviting submissions: Anindilyakwa Land Council, Tiwi Land Council, Northern Land Council, Central Land Council, Auditor-General of Australia, National Workplace Relations Consultative Council, Reserve Bank of Australia, Export and Finance Insurance Corporation, Classification Review Board, Office of Film and Literature Classification, and Austrade. The ALRC has not received any submissions from these agencies.

107 There are only four exemptions in the *Data Protection Act 1998* (UK) and three in *Personal Data (Privacy) Ordinance* (Hong Kong): see *Data Protection Act 1998* (UK) ss 30(2), 30(3), 31, 36; *Personal Data (Privacy) Ordinance* (Hong Kong) ss 52, 57, 61; and Ch 33.

AUSTRAC

36.77 The current partial exemption that applies to AUSTRAC should remain. The exemption is a limited one and does not apply to AUSTRAC's administrative activities. The application of the UPPs to AUSTRAC's existing exempt activities may cause difficulties for its operation, particularly the 'Collection', 'Notification' and 'Anonymity and Pseudonymity' principles. In addition, the handling of information by AUSTRAC is governed by PSM 2005 and ACSI 33, as well as a secrecy provision that prohibits AUSTRAC officials from disclosing information collected, compiled or analysed by AUSTRAC. Unlike the other agencies listed in sch 2 of the FOI Act, the functions of AUSTRAC are more akin to those of law enforcement agencies. For these reasons, AUSTRAC should remain partially exempt from the operation of the *Privacy Act*.

ABC and SBS

36.78 The ABC and the SBS should not be exempt from the *Privacy Act* by virtue of their exempt status under the FOI Act. There are insufficient policy justifications for treating national broadcasters differently to media organisations in the private sector for the purposes of the *Privacy Act*. Setting aside the question of access and correction to their records, which is generally dealt with under the FOI Act, there is no justification for a specific exemption for the ABC and the SBS in relation to their program materials and datacasting content.

36.79 Both the ABC and the SBS submitted that they should be exempt in relation to their programming materials because they are not in commercial competition with private sector media organisations. While it is arguable whether the ABC and the SBS are in commercial competition with other media organisations, as agencies, the national broadcasters should be required to comply with the *Privacy Act* unless there is a clear policy justification for their exemption. In the case of the ABC and the SBS, the relevant policy justification is the public interest in promoting freedom of expression in the context of their journalistic activities—the same public interest consideration that applies to other media organisations. Therefore, the ABC and the SBS should be treated consistently with other media organisations, which are exempt in relation to acts done, or practices engaged in, in the course of journalism.[108] Applying the journalism exemption to the national broadcasters also would ensure that their independence and integrity in the context of their journalistic activities is preserved.

36.80 The ALRC notes the concern raised by the ABC that the removal of its partial exemption may result in it being excluded from the journalism exemption, on the basis that its programming activities are not 'commercial activities'. To the extent that the ABC and the SBS's programming activities are considered non-commercial activities,

---

108 See Ch 42.

s 7A of the *Privacy Act* will not apply to deem the ABC or the SBS to be an 'organisation' and therefore not a 'media organisation' in relation to its programming activities. To address this concern, the ALRC recommends in Chapter 42 that the ABC and the SBS be prescribed by regulations as 'media organisations' for the purposes of the journalism exemption.[109] In addition, the ALRC recommends that the removal of their partial exemption from the operation of the *Privacy Act* should be conditional upon their being prescribed by regulations as 'media organisations'. This will ensure that the ABC and the SBS are not placed at a disadvantage upon the removal of their partial exemption.

36.81 The ALRC also notes the submission by the ABC that empowering the Privacy Commissioner to deal with privacy complaints in relation to the ABC's programming activities would reduce the ABC Board's oversight of such activities and interfere with the role of ACMA in dealing with privacy-related complaints against the ABC. This concern is addressed adequately by recommendations made by the ALRC elsewhere in this Report. As mentioned above, the ALRC is recommending that the ABC and the SBS be prescribed by regulations as 'media organisations' for the purposes of the journalism exemption. Accordingly, the ABC and the SBS's programming activities generally would be covered by the journalism exemption and therefore fall outside the jurisdiction of the Privacy Commissioner.

36.82 For programming activities of the ABC and the SBS that do not fall within the scope of the journalism exemption, the ALRC accepts that both ACMA and the Privacy Commissioner would have jurisdiction to hear privacy-related complaints concerning such activities. In Chapter 73, the ALRC recommends that the OPC, ACMA and the Telecommunications Industry Ombudsman should develop memorandums of understanding addressing several issues, including: the roles and functions of each of the bodies under the *Privacy Act* and other legislation; the exchange of relevant information and expertise between the bodies; and when a matter should be referred to, or received from, the bodies.[110] Such memorandums of understanding would ensure that there is greater cooperation between the OPC and ACMA when dealing with privacy-related complaints against media organisations.

36.83 In addition, the ALRC notes that the Privacy Commissioner currently has power not to investigate, or not to investigate further, complaints in defined circumstances, including where the complaint has been, or is being dealt with, adequately under another law.[111] The ALRC also recommends in Chapter 49 that the Privacy Commissioner should be given more discretion not to investigate individual complaints in certain circumstances, including where an investigation, or a further investigation, is not warranted having regard to all the circumstances.[112] These powers would allow the OPC to decide not to investigate a complaint that is being considered by ACMA. The

---

109 See Rec 42–2.
110 See Rec 73–8.
111 *Privacy Act 1988* (Cth) s 41.
112 Rec 49–1.

ALRC is therefore satisfied that regulatory oversight of the ABC and the SBS by the Privacy Commissioner would not interfere with ACMA's role in dealing with privacy-related complaints against them.

FOI exemption

36.84 Currently, the ABC, the SBS and the other agencies discussed above are either partially or completely exempt from the operation of the FOI Act.[113] In Chapter 29, the ALRC recommends that the right of access to personal information held by an agency should be subject to the applicable provisions of any Commonwealth law.[114] Therefore, the right of access to personal information held by agencies that are exempt from the operation of the FOI Act will continue to be subject to the FOI Act. The appropriateness of the exemption of these agencies from the FOI Act currently is the subject of a separate inquiry on the FOI Act being conducted by the ALRC. The ALRC therefore makes no recommendations on this issue.

Recommendation 36–2 The following agencies listed in Schedule 2, Part I, Division 1 and Part II, Division 1 of the *Freedom of Information Act 1982* (Cth) should be required to demonstrate to the minister responsible for administering the *Privacy Act* that they warrant exemption from the operation of the *Privacy Act*:

(a) Aboriginal Land Councils and Land Trusts;

(b) Auditor-General;

(c) National Workplace Relations Consultative Council;

(d) Department of the Treasury;

(e) Reserve Bank of Australia;

(f) Export and Finance Insurance Corporation;

(g) Australian Communications and Media Authority;

(h) Classification Board;

(i) Classification Review Board; and

113 *Freedom of Information Act 1982* (Cth) s 7.
114 See Rec 29–2.

(j) Australian Trade Commission.

The Australian Government should remove the exemption from the operation of the *Privacy Act* for any of these agencies that, within 12 months from the tabling of this Report, do not make an adequate case for retaining their exempt status.

Recommendation 36–3 The *Privacy Act* should be amended to remove the partial exemption that applies to the National Health and Medical Research Council.

Recommendation 36–4 Subject to the implementation of Recommendation 42–2 (regulations specifying agencies, including the Australian Broadcasting Corporation and the Special Broadcasting Service, as 'media organisations' under the *Privacy Act*), the *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Broadcasting Corporation and the Special Broadcasting Service.

37. Agencies with Law Enforcement Functions

Contents

Introduction

37.1 Most agencies with law enforcement functions are covered by the *Privacy Act 1988* (Cth), although a number of exceptions to the Information Privacy Principles (IPPs) exist for law enforcement activities. Two law enforcement agencies, however, are exempt specifically from the operation of the *Privacy Act*—namely, the Australian Crime Commission (ACC), and the Integrity Commissioner and staff members of the Australian Commission for Law Enforcement Integrity (ACLEI). This chapter considers whether these exemptions are justified and whether law enforcement activities should be included in the *Privacy Act* by way of an exemption rather than exceptions.[1]

1 This distinction between an 'exception' and an 'exemption' is discussed below.

Australian Crime Commission

Background

37.2 Organised crime is recognised as a major threat to individuals and to society. In adopting the *United Nations Convention against Transnational Organized Crime*, the main international instrument relied upon to combat such activity, the General Assembly of the United Nations stated that it was:

> *Deeply concerned* by the negative economic and social implications related to organized criminal activities, and was convinced of the urgent need to strengthen cooperation to prevent and combat such activities more effectively at the national, regional and international levels.[2]

37.3 Organised crime groups are involved in a diverse range of criminal activities, including drug trafficking, corruption, violence, fraud, money laundering and other financial sector crimes.[3] These groups are influential and have significant resources and capability to resist law enforcement. They tend to utilise sophisticated methods and techniques that target weaknesses in individuals, agencies, organisations and industries. For example, organised crime groups often gather intelligence about those they seek to influence—including businesses, public officials and law enforcement officers—through the use of corruption, intimidation, extortion, or implied or actual violence. They also may protect themselves by disguising their identity and laundering proceeds of crime to conceal the origin of those proceeds.[4]

37.4 To counter serious and organised crime in Australia, the ACC was established under the *Australian Crime Commission Act 2002* (Cth) (ACC Act). The ACC was formed by replacing the National Crime Authority (NCA), and absorbing the functions of the Australian Bureau of Criminal Intelligence (ABCI)[5] and the Office of Strategic Crime Assessments.[6] The functions of the ACC include: collecting and analysing criminal intelligence; setting national criminal intelligence priorities; providing and

---

2 *United Nations Convention against Transnational Organized Crime*, 12 December 2000, [2004] ATS 12, (entered into force generally on 29 September 2003). The Convention was ratified by the Australian Government on 27 May 2004 and entered into force for Australia on 26 June 2004.

3 Ibid; United Nations on Drugs and Crime, *UNODC and Organized Crime* <www.unodc.org> at 27 March 2008; Australian Crime Commission, *Organised Crime in Australia* (2008), 4.

4 Australian Crime Commission, *Organised Crime in Australia* (2008), 4–6, 13.

5 The ABCI was established to facilitate the exchange of criminal intelligence among federal, state and territory law enforcement agencies, anti-corruption bodies and regulatory agencies. It was responsible for the analysis and dissemination of criminal intelligence, but relied on these agencies for the collection of information: Australian Crime Commission, *Annual Report 2002–2003* (2003), 152; Parliament of Australia—Parliamentary Joint Committee on the Australian Crime Commission, *The Law Enforcement Implications of New Technology* (2001).

6 The Office of Strategic Crime Assessments was an element of the Australian Government Attorney-General's Department preparing national level strategic law enforcement intelligence: Australian Crime Commission, *Submission to the Inquiry by the Parliamentary Joint Committee of Public Accounts and Audit Management and Integrity of Electronic Information in the Commonwealth*, 1 January 2003, 4.

maintaining criminal intelligence systems; and investigating federally relevant criminal activity and undertaking taskforces.[7]

37.5 Although the ACC falls within the definition of 'agency' under the *Privacy Act*, the acts and practices of the ACC are excluded from the reference to 'an act or practice' in the Act.[8] In addition, s 7(2) of the Act exempts the ACC from compliance with the tax file number provisions of the Act. The ACC, therefore, is completely exempt from the operation of the Act.

37.6 Acts and practices in relation to records that have originated with, or have been received from, the ACC or the Board of the ACC (ACC Board) also are exempt.[9] Accordingly, agencies and organisations receiving a record from the ACC are exempt from the operation of the *Privacy Act* in relation to that record. Furthermore, since the ACC falls within the definition of an 'enforcement body' under the Act,[10] personal information may be disclosed by an organisation to the ACC in defined circumstances, including where the disclosure is reasonably necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences; or the prevention, detection, investigation or remedying of seriously improper conduct.[11]

37.7 The ACC may conduct its investigations or operations through the use of a range of law enforcement powers, including the application for search warrants, participation in controlled operations, use of surveillance devices, interception of telecommunications, access to stored communications and use of assumed identities.[12] In addition, the ACC has a range of special powers that are used 'where ordinary law enforcement methodologies are ineffective'.[13] These include the power to conduct examinations, issue a summons requiring a person to attend an examination to give evidence under oath or affirmation, and requiring the production of any document or thing.[14] Failure to attend an examination, or to answer questions or produce specified documents or things at an examination, are offences that are punishable by fines and imprisonment.[15]

---

7 Australian Crime Commission, *Australian Crime Commission Profile* (2008) <www.crimecommission.gov.au/content/about/ACC_PROFILE.pdf> at 27 March 2008, 1.

8 *Privacy Act 1988* (Cth) s 7(1)(a)(iv).

9 Ibid s 7(1)(h).

10 Ibid s 6(1).

11 Ibid sch 3 NPP 2.1(h).

12 *Australian Crime Commission Act 2002* (Cth) s 22; *Crimes Act 1914* (Cth) ss 15J, 15XB; *Surveillance Devices Act 2004* (Cth) pts 2–4; *Telecommunications (Interception) Act 1979* (Cth) ss 39, 110.

13 Australian Crime Commission, *Australian Crime Commission Profile* (2008) <www.crimecommission.gov.au/content/about/ACC_PROFILE.pdf> at 27 March 2008, 1.

14 *Australian Crime Commission Act 2002* (Cth) pt II div 2.

15 Ibid s 30.

37.8 The ACC Act contains a secrecy provision that prohibits ACC officials and staff from recording, communicating or divulging any information acquired by reason, or in the course, of the performance of their duties under the Act.[16]

37.9 There is tension between privacy and law enforcement, particularly in the context of organised crime. As noted by Dr Chris Corns:

> By definition, effective law enforcement and investigation of organised crime requires maximum disclosure of information by government departments to law enforcement agencies. In theory, a maximum flow of information between law enforcement agencies is also required. At the same time, governments have an interest in preventing the unjustified or unnecessary disclosure of information and protecting citizens from unjustified invasions of their privacy by state officials.[17]

37.10 In a recent review of the ACC Act, the Parliamentary Joint Committee on the ACC commented that:

> Given the particularly violent and pernicious nature of organised crime, history has shown the need to create specialist crime fighting bodies with significant powers to combat these organised crime networks. However, it is evident from the description of the ACC's powers … that the actions of the ACC have the potential to impact profoundly on the individual citizen's freedom and privacy.[18]

Information management guidelines

37.11 The primary documents that prescribe the requirements for the management and security of information by the ACC include the *Protective Security Manual* (PSM 2005), the *Australian Government Information and Communications Technology Security Manual* (ACSI 33) and the *ACC Policy and Procedures Manual*.[19] The *ACC Policy and Procedures Manual* is a classified document.[20]

37.12 The PSM 2005 is a policy document that sets out guidelines and minimum standards in relation to protective security for agencies and officers. It also applies to contractors and their employees who perform services for the Australian Government. In particular, Part C provides guidance on the classification system and the protective standards required to protect both electronic and paper-based security classified

---

16 Ibid s 51. The section applies to the Chief Executive Officer of the ACC, members of the ACC Board, members of the ACC staff and examiners. *Australian Crime Commission Act 2002* (Cth) ss 24A, 46B.

17 C Corns, 'Inter Agency Relations: Some Hidden Obstacles to Combating Organised Crime?' (1992) 25 *Australia and New Zealand Journal of Criminology* 169, 177.

18 Parliament of Australia—Parliamentary Joint Committee on the Australian Crime Commission, *Review of the Australian Crime Commission Act 2002* (2005), [5.86].

19 Australian Crime Commission, *Submission to the Inquiry by the Parliamentary Joint Committee of Public Accounts and Audit Management and Integrity of Electronic Information in the Commonwealth*, 1 January 2003, 11. The ACC also is required to comply with *Australian Government Standards for the Protection of Information Technology Systems Processing Non-National Security Information at the Highly Protected Classification* (ACSI 37) published by the DSD. ASCI 37 is a controlled document that outlines certain requirements for physical security.

20 In addition, there is a range of state legislative and guidance documents prescribing the ACC's requirements for the management and security of information entrusted to the ACC: Ibid, 11.

information.[21] The part sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information.

37.13 Agencies also are required by the PSM 2005 to comply with the ACSI 33, which has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to agencies on the protection of their electronic information systems.[22]

Accountability and oversight mechanisms

37.14 The ACC is subject to oversight through a number of mechanisms described below.

Ministerial oversight

37.15 The ACC currently is responsible to the Minister for Home Affairs.[23] The Chair of the ACC Board must keep the Minister informed of the general conduct of the ACC in the performance of its functions and comply with the Minister's request for information concerning any specific matter relating to such conduct.[24] The Minister also may give directions or issue guidelines to the ACC Board in relation to the performance of the Board's functions.[25]

ACC Board

37.16 The ACC Board consists of the Commissioner of the Australian Federal Police (AFP), the Secretary of the Attorney-General's Department (AGD), the Chief Executive Officer (CEO) of the Australian Customs Service, the Chairperson of the Australian Securities and Investments Commission (ASIC), the Director-General of Security, eight state and territory police commissioners, and the CEO of the ACC (as a non-voting member).[26]

37.17 The Board's functions include:

- determining national criminal intelligence priorities;
- authorising the ACC to undertake intelligence operations or to investigate matters relating to federally-relevant criminal activity;

---

21 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 8 April 2008.

22 Australian Government Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual (ACSI 33)* (2007).

23 Australian Crime Commission, *Australian Crime Commission Profile* (2008) <www.crimecommission.gov.au/content/about/ACC_PROFILE.pdf> at 27 March 2008.

24 *Australian Crime Commission Act 2002* (Cth) s 59.

25 Ibid s 18.

26 Ibid ss 7B, 7G(3).

- determining whether an operation or investigation is a special operation or investigation;[27]
- determining the classes of persons to participate in an intelligence operation or investigation;
- establishing task forces;
- disseminating strategic criminal intelligence assessments to law enforcement agencies, foreign law enforcement agencies, or prescribed federal, state or territory agencies; and
- reporting to the Inter-Governmental Committee on the ACC's performance.[28]

Inter-Governmental Committee

37.18 The Inter-Governmental Committee on the ACC (IGC) consists of the Minister for Home Affairs, and federal, state and territory police or justice ministers.[29] It was established under the ACC Act to: monitor the work of the ACC and the ACC Board; oversee the strategic direction of the ACC and the ACC Board; and receive reports from the Board for transmission to federal, state and territory governments.[30] Where the ACC Board has determined that an investigation or operation is a special investigation or operation, the IGC may request that the Chair of the ACC Board provide the IGC with further information in relation to the determination.[31] The IGC also has the power to revoke that determination.[32]

---

27 The ACC Board may determine that an intelligence operation is a special operation if it considers that methods of collecting criminal information and intelligence that do not involve the use of powers in the ACC Act have not been effective: Ibid s 7C(2). The Board may determine that an investigation into matters relating to federally relevant criminal activity is a special investigation if it considers that ordinary police methods of investigation into the matters are unlikely to be effective: s 7C(3). The making of such a determination by the ACC Board allows an eligible person within the ACC to apply for search warrants; or an ACC examiner to apply to the Federal Court for the surrender of a passport, conduct examinations, summon a person to attend an examination, require a person to produce documents or other things, or apply to the Federal Court for a warrant where a witness fails to surrender a passport: ss 22–25A, 28, 29, 31.

28 Ibid s 7C(1).

29 Ibid s 8(1).

30 Ibid s 9(1).

31 Ibid s 9(2). The Chair of the ACC Board only may refuse to give that information if it considers that the disclosure of the information to the public could prejudice the safety or reputation of persons or the operation of the law enforcement agencies. If the information is withheld on this ground, the IGC may refer its request to the Minister for his or her determination: *Australian Crime Commission Act 2002* (Cth) s 9(3), (6).

32 *Australian Crime Commission Act 2002* (Cth) s 9(7).

Parliamentary Joint Committee

37.19 The Parliamentary Joint Committee on the ACC comprises members from both the Senate and the House of Representatives.[33] It is responsible for:

- monitoring and reviewing the performance of the ACC;
- reporting to the Parliament in relation to the ACC;
- examining the ACC's annual reports;
- examining trends and changes in criminal activities, practices and methods;
- recommending changes to the functions, structure, powers and procedures of the ACC to the Parliament; and
- conducting inquiries.[34]

Commonwealth Ombudsman

37.20 Under the *Ombudsman Act 1976* (Cth), the Commonwealth Ombudsman has the power to investigate complaints against the ACC that relate to matters of administration.[35] It also has oversight of the ACC's use of controlled operations under Part IAB of the *Crimes Act 1914* (Cth), surveillance devices under the *Surveillance Devices Act 2004* (Cth) and state and territory surveillance device laws, and telephone intercept and stored communications warrants under the *Telecommunications (Interception) Act 1979* (Cth).[36]

37.21 In 2006–07, the Commonwealth Ombudsman received nine complaints about the ACC,[37] three of which were within its jurisdiction.[38] One complaint was referred to the ACC, which appointed an independent officer to investigate. No evidence of misconduct by ACC officers was found. Another complaint was investigated by the Ombudsman, who decided not to take any further action as he was satisfied that the

---

33 Ibid s 53.

34 Ibid s 55.

35 *Ombudsman Act 1976* (Cth) ss 3(13A), 5(1).

36 *Crimes Act 1914* (Cth) s 15UB; *Surveillance Devices Act 2004* (Cth) s 55; *Telecommunications (Interception) Act 1979* (Cth) ss 83, 152. A 'controlled operation' is an operation that: involves the participation of law enforcement officers; is carried out for the purpose of obtaining evidence in relation to a serious Commonwealth offence or a serious state offence that has a federal aspect; and may involve a law enforcement officer or other person in acts or omissions that would constitute an offence: *Crimes Act 1914* (Cth) s 15H.

37 Commonwealth Ombudsman, *Annual Report 2006–2007* (2007), 96. This is the same number of complaints against the ACC as in 2005–06: Commonwealth Ombudsman, *Annual Report 2005–2006* (2006), 91.

38 The Commonwealth Ombudsman stated that some of the other complaints were from people seeking to report criminal activity and the Ombudsman gave them the contact details of the ACC: Commonwealth Ombudsman, *Annual Report 2006–2007* (2007), 96.

ACC had already provided an appropriate remedy to the complainant. The Ombudsman decided not to investigate the third complaint, on the basis that an investigation into matters that have allegedly occurred many years ago was 'problematic' and 'unlikely to achieve the remedy sought by the complainant'.[39] In 2007, the Ombudsman also referred an allegation of corruption related to the ACC to the ACLEI.[40]

37.22 The Commonwealth Ombudsman inspected the records of the ACC on six occasions in 2006–07, and concluded that there was general compliance with legislative requirements by the ACC. The Ombudsman also reported that his recommendations to improve record keeping were generally accepted by the ACC, which has since implemented measures to improve record keeping and procedures.[41]

Australian Commission for Law Enforcement Integrity

37.23 The Integrity Commissioner, supported by the ACLEI, is responsible for preventing, detecting and investigating serious corruption issues in agencies with law enforcement functions, including the ACC.[42] The functions of the Integrity Commissioner include, among other things, investigating and reporting on corruption issues, conducting public inquiries into corruption, and handling information and intelligence relating to corruption.[43]

Auditor-General

37.24 The Auditor-General is an independent officer of the Australian Parliament responsible for performing financial and performance audits of certain agencies, including the ACC.[44] The Auditor-General has broad information-gathering powers and authority to have access to Commonwealth premises.[45]

Discussion Paper proposal

37.25 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC considered how best to accommodate the law enforcement functions of the ACC. The ALRC noted the Office of the Privacy Commissioner (OPC) submission that the exemption that applies to the ACC originally applied to the NCA, and that the reasons behind the exemption that applied originally to the NCA

---

39 Ibid, 96–97.

40 Ibid, 97. See also Australian Commission for Law Enforcement Integrity, *Annual Report of the Integrity Commissioner 2006–07* (2007), 23.

41 Commonwealth Ombudsman, *Annual Report 2006–2007* (2007), 109–110.

42 *Law Enforcement Integrity Commissioner Act 2006* (Cth) ss 5(1) (definition of 'law enforcement agency'), 7, 15. At present, the Act only applies to the ACC, Australian Federal Police and the former NCA.

43 Ibid s 15.

44 *Auditor-General Act 1997* (Cth) ss 11, 15, 18; *Financial Management and Accountability Act 1997* (Cth) s 5; *Financial Management and Accountability Regulations 1997* (Cth) sch 1 pt 1 item 108A.

45 *Auditor-General Act 1997* (Cth) pt 5 div 1.

> appear to have been based on the NCA's coercive powers, unique to Commonwealth law enforcement, which allowed the collection of personal information of a speculative and untested nature.[46]

37.26 The OPC submitted that, since the absorption of the ABCI's functions into the ACC, much of the information collected by the former ABCI is now collected and stored on the ACC's intelligence databases. In addition, the OPC observed that many of the records held in these databases are sourced from the AFP, Australian Transaction Reports and Analysis Centre (AUSTRAC), ASIC and other agencies that are covered by the *Privacy Act*. The OPC also stated that some agencies that perform a law enforcement function are covered by the *Privacy Act*, and that it has issued guidance on how the Act provides for law enforcement needs.[47] The OPC submitted that 'in view of the changed role of the ACC over the years … it may be timely to reassess the suitability of the current ACC exemption from the *Privacy Act*'. The OPC suggested that 'one option [for reform] could be for the administrative operations of the ACC to be covered by the *Privacy Act*'.[48]

37.27 In another submission, it was suggested that the ACC should be partially exempt from the *Privacy Act*, but only on a case-by-case basis and where there is sufficient oversight.[49]

37.28 The ALRC considered three options for reform in DP 72. One option would be to remove the exemption that applies to the ACC and rely on its inclusion in the definition of 'enforcement body' under the *Privacy Act*. This would ensure that the ACC is subject to the privacy principles except to the extent that non-compliance is required for the performance of its law enforcement activities. In the United Kingdom, for example, the Serious Organised Crime Agency is not exempt from compliance with the *Data Protection Act 1998* (UK), but relies on exceptions under that Act for its operations.[50]

37.29 Another option would be to modify the exemption so that the ACC is covered by the *Privacy Act* in respect of its administrative operations, such as the handling of its employee records, but otherwise is exempt. For instance, the New South Wales Crime Commission is exempt from compliance with the *Privacy and Personal Information Protection Act 1998* (NSW) except in connection with the exercise of its administrative and educative functions.[51]

---

46 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

47 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 28.

48 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

49 K Handscombe, *Submission PR 89*, 15 January 2007.

50 Section 29 of the *Data Protection Act 1998* (UK) relevantly provides that data controllers do not have to comply with certain data protection principles where the personal data are processed for the purposes of, among other things, the prevention or detection of crime, or the apprehension or prosecution of offenders. See also *Serious Organised Crime and Police Act 2005* (UK) s 33(4).

51 *Privacy and Personal Information Protection Act 1998* (NSW) s 27.

37.30 A third option would be to require the ACC to comply with information-handling guidelines, to be developed in consultation with the OPC and issued by the Minster for Home Affairs. This approach is similar to the approach taken in relation to exempt defence and intelligence agencies, which are still required to comply with ministerial directions or guidelines in relation to privacy.[52] In its 2007 report, *Inquiry into the Future Impact of Serious and Organised Crime on Australian Society*, the Parliamentary Joint Committee on the ACC observed that the adoption by the ACC of information-handling protocols would be an appropriate means of ensuring the protection of intelligence data handled by the ACC. The Committee therefore recommended that the ACC 'give consideration to the extent to which its information handling protocols incorporate, and could be enhanced by, the principles of the *Privacy Act*'.[53]

37.31 In DP 72, the ALRC observed that the ACC already is subject to information management guidelines and a substantial amount of oversight. The ALRC noted, however, that there is significant potential for the ACC's activities to affect the privacy of individuals. The ALRC also noted that the ACC's exempt status is anomalous with the position of other federal law enforcement agencies, which are covered by the *Privacy Act*. In addition, many of the records held in the ACC's databases are collected from the AFP, AUSTRAC, ASIC and other agencies that already are covered by the *Privacy Act*.

37.32 The ALRC expressed the preliminary view that there are several specific exceptions to the IPPs that allow federal law enforcement agencies to carry out their law enforcement functions, and that the proposed Unified Privacy Principles (UPPs) also contain a number of specific exceptions that would allow those agencies to function effectively. The ALRC therefore proposed that the *Privacy Act* be amended to remove the exemption that applies to the ACC and the ACC Board by repealing s 7(1)(a)(iv), (h) and 7(2) of the Act.[54]

Submissions and consultations

37.33 Some stakeholders supported the proposal to remove the exemption for the ACC and the ACC Board.[55] The Cyberspace Law and Policy Centre argued that the ACC should be required to justify any exemption from both the *Privacy Act* and the related provisions of the *Freedom of Information Act 1982* (Cth) (FOI Act), and that 'no agency should be wholly exempt from the obligation to comply with fundamental human rights and administrative law principles'. It also suggested that, where an

52 See discussion in Ch 34.

53 Australian Parliament—Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into the Future Impact of Serious and Organised Crime on Australian Society* (2007), [8.51], rec 20.

54 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 34–2.

55 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

exemption is justified, information-handling guidelines should be developed and published in consultation with the OPC.[56]

37.34 The Public Interest Advocacy Centre (PIAC) noted that the activities of the ACC may have a significant impact on the privacy of individuals, and that the exemption for the ACC is anomalous with the position of other federal law enforcement agencies.[57] Stakeholders also argued that current privacy regulation and exceptions to the privacy principles allow for the specific needs of law enforcement and should be sufficient to enable the ACC to function effectively.[58]

37.35 The OPC submitted that entities with like functions should be treated consistently under the *Privacy Act* and that other Australian law enforcement agencies, such as the AFP and AUSTRAC, are covered by the *Privacy Act*. The exemption that applies to the ACC could therefore be considered 'an irregularity' and maintaining it 'may create a break in the continuity of privacy protections'.[59]

37.36 The OPC submitted that personal information sourced from enforcement agencies that are covered by the *Privacy Act* would fall outside the scope of the Act once it is held on the ACC's records, including records held in the Australian Criminal Intelligence Database, which is used by all Australian police forces and many other agencies.[60]

37.37 Two stakeholders did not support the proposal to remove the exemption that applies to the ACC and the ACC Board. The AFP submitted that the original policy reasons for the exemption continue to apply, and that the ACC has limited functions and strict secrecy provisions that obviate the need for it to be subject to the *Privacy Act*.[61]

37.38 The ACC submitted that it is generally accepted that the public interest in combating organised crime outweighs an individual's right to privacy. It suggested that the ACC is distinguishable from other law enforcement agencies in that the ACC has greater coercive information-gathering powers that are similar to those of Royal Commissions. Such powers, it argued, are justified because of the complex and sophisticated organisational structure and operations of organised crime groups, and the substantial resources such groups have at their disposal.[62]

---

56 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
57 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
58 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.
59 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
60 Ibid.
61 Australian Federal Police, *Submission PR 545*, 24 December 2007.
62 Australian Crime Commission, *Correspondence*, 8 May 2008.

37.39 The ACC further advised that applying the *Privacy Act* to the ACC would adversely affect the effectiveness of its investigations and operations for two reasons. First, the ACC's access to coercive powers that may impinge upon the privacy of individuals is necessary to allow it to lawfully obtain information that is unavailable by other means and therefore is central to the effectiveness of its operations. It argued that the requirements of the *Privacy Act* would be incompatible with the ACC's exercise of these coercive powers.[63]

37.40 Secondly, subjecting the ACC to complaint, investigation and review procedures under the *Privacy Act* could result in difficulties in obtaining evidence from some witnesses, and in encouraging agencies to share criminal intelligence. The ACC suggested that, given it is already subject to extensive internal and external oversight mechanisms, review by another external body like the OPC would result in a perceived weakening of the secrecy regime under the ACC Act and discourage witnesses from cooperating with the ACC.[64]

37.41 In addition, the ACC suggested that there already is sufficient regulation of the way it handles personal information, including secrecy provisions, non-publication orders imposed by ACC examiners and other legislation (such as the *Surveillance Devices Act* and the *Telecommunications (Interception and Access) Act*), and extensive internal and external oversight of the ACC's activities. Information obtained by the ACC also is subject to special protection when it is passed on to other agencies—the classification and conditions of use for that material is specified by the ACC and the recipient of the information is required to seek the approval of the ACC for any additional use.[65]

37.42 Finally, the ACC submitted that partially exempting it from the operation of the *Privacy Act* would be unworkable, because the need to ensure high standards of integrity of ACC staff means that sensitive information obtained by the ACC on current and prospective staff should not be made available to the individual staff members concerned. It argued that denying access to personal information requested by a particular ACC staff member in a particular case could alert the individual to the fact that he or she is under suspicion and impede the effective investigation of that individual by the ACC or the ACLEI.[66]

ALRC's view

37.43 As the discussion in Chapter 1 illustrates, the right to privacy is not absolute. Privacy interests must be balanced with other competing public interests, including 'the need of society to create and enforce rules of personal and corporate behaviour for the

63 Ibid.
64 Ibid.
65 Ibid.
66 Ibid.

common good'.[67] Due to the insidious and particularly violent nature of organised crime, the ACC has been given significant coercive information-gathering powers, including traditional law enforcement powers, such as covert intelligence gathering and surveillance. The ACC also has been given powers that are not available to other law enforcement agencies, such as the power to conduct examinations.[68] As recognised by the Parliamentary Joint Committee on the ACC, it is clear that the ACC's activities can have a significant impact on the privacy of individuals. There is a need, therefore, to ensure that personal information handled by the ACC is protected adequately.

37.44 The *Privacy Act*, however, may not be the appropriate mechanism to address privacy issues relating to the ACC. First, the powers of the ACC are required to be exercised in a confidential manner to protect the integrity of its investigations, as well as the privacy and safety of witnesses and other persons assisting the ACC.[69] Given the sensitive nature of the ACC's operations, the OPC may not be the appropriate body to deal with complaints against the ACC. Secondly, a separate system of oversight and accountability has been established specifically to ensure that the ACC exercises its powers appropriately while maintaining the appropriate balance between secrecy and accountability. Any privacy issues relating to the ACC should be monitored through this separate system.

37.45 The ALRC, therefore, has come to the view that the ACC and the ACC Board should remain exempt from the operation of the *Privacy Act*, provided that they are subject to information-handling guidelines to be developed and published in consultation with the OPC. In the ALRC's view, these guidelines should correspond with the model UPPs as closely as possible. Compliance with the information-handling guidelines should be overseen by the Parliamentary Joint Committee on the ACC, the main external body responsible for monitoring the ACC in the performance of its functions.

37.46 To address the OPC's concern that information, once held on the ACC's records, could result in a break in the continuity of privacy protection, the information-handling guidelines should address the conditions to be imposed on the recipients of personal information disclosed by the ACC in relation to the further handling of that information. In addition, the information-handling guidelines should address whether an appropriate complaint-handling mechanism for privacy-related complaints that do not fall under the jurisdiction of the Commonwealth Ombudsman or the Integrity Commissioner needs to be established.

---

67 Parliament of Australia—Parliamentary Joint Committee on the Australian Crime Commission, *Review of the Australian Crime Commission Act 2002* (2005), [5.85].

68 Australian Crime Commission, *Organised Crime in Australia* (2008), 13.

69 M Irwin, 'Policing Organised Crime' (Paper presented at 4th National Outlook Symposium on Crime in Australia: New Crimes or Responses, Canberra, 21–22 June 2001), 8.

Recommendation 37–1 (a) The Australian Crime Commission (ACC), in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for the ACC and the Board of the ACC. The information-handling guidelines should address the conditions to be imposed on the recipients of personal information disclosed by the ACC in relation to the further handling of that information.

(b) The Parliamentary Joint Committee on the ACC should monitor compliance by the ACC and the Board of the ACC with the information-handling guidelines.

Integrity Commissioner

Background

37.47 Corruption is a serious global phenomenon that undermines democratic institutions, jeopardises economic development, and threatens the stability and security of governments.[70] While there is no universally accepted definition of corruption, it is understood to include bribery, embezzlement, extortion, illicit enrichment, and abuse of functions, position or influence.[71]

37.48 The seriousness of the threat posed by corruption has been recognised by the General Assembly of the United Nations, which adopted the *United Nations Convention against Corruption* on 31 October 2003. The Convention requires that parties to the Convention ensure the existence of independent anti-corruption bodies that implement measures to prevent and combat corruption, and, in particular, 'a body, bodies or persons specialised in combating corruption through law enforcement' that are independent and free from any undue influence.[72]

37.49 Commencing operation in December 2006, the ACLEI was established to detect and investigate corruption in the AFP, the ACC, the former NCA and prescribed Australian Government agencies with law enforcement functions.[73] It is headed by the Integrity Commissioner, whose functions include:

- investigating and reporting on corruption issues;

---

70 See *United Nations Convention against Corruption*, 9 December 2003, [2006] ATS 2, (entered into force generally on 14 December 2005), Preamble. The Convention was ratified by the Australian Government on 7 December 2005 and entered into force for Australia on 6 January 2006.

71 See Ibid, arts 15–22. See also United Nations Office on Drugs and Crime, *United Nations Guide on Anti-Corruption Policies* (2003), 28–34.

72 See *United Nations Convention against Corruption*, 9 December 2003, [2006] ATS 2, (entered into force generally on 14 December 2005), arts 6, 36.

73 *Law Enforcement Integrity Commissioner Act 2006* (Cth) ss 5(1) (definition of 'law enforcement agency'), 7, 15. No additional Australian Government agencies have yet been prescribed as law enforcement agencies under the Act.

- referring corruption issues to law enforcement agencies for investigation;
- managing, overseeing or reviewing the investigation of corruption by law enforcement agencies;
- conducting public inquiries into corruption;
- collecting, analysing and communicating information and intelligence relating to corruption; and
- making reports and recommendations to the responsible minister concerning the need or desirability of legislative or administrative actions on corruption issues.[74]

37.50 The ACLEI may conduct investigations through the use of various law enforcement powers, including the application for, and execution of, arrest and search warrants, participation in controlled operations, use of surveillance devices, interception of telecommunications, access to stored communications and use of assumed identities.[75] Additionally, the Integrity Commissioner has similar powers to a Royal Commission, including the power to execute search warrants, conduct public or private hearings, summon people to attend hearings to give evidence or produce any document or thing, and take possession of, copy or retain any document or thing.[76]

37.51 The Integrity Commissioner is exempt from the operation of the *Privacy Act*.[77] Acts and practices in relation to a record that has originated with, or has been received from, the Integrity Commissioner or a staff member of the ACLEI, also are exempt.[78] In addition, since the Integrity Commissioner is an 'enforcement body' under the Act,[79] personal information may be disclosed by an organisation to the Integrity Commissioner in certain circumstances, including where the disclosure is for the purpose of preventing, detecting, investigating or prosecuting criminal offences, or the prevention, detection, investigation or remedying of seriously improper conduct.[80]

37.52 The *Law Enforcement Integrity Commissioner Act 2006* (Cth) (LEIC Act) imposes certain confidentiality requirements on the ACLEI staff.[81] A current or former ACLEI staff member must not record, divulge or communicate any information

---

74 Ibid s 15.
75 Ibid ss 99, 108; *Crimes Act 1914* (Cth) ss 15J, 15XB; *Surveillance Devices Act 2004* (Cth) pts 2–4; *Telecommunications (Interception) Act 1979* (Cth) ss 39, 110.
76 *Law Enforcement Integrity Commissioner Act 2006* (Cth) pt 9.
77 *Privacy Act 1988* (Cth) s 7(1)(a)(iiia).
78 Ibid s 7(1)(ga).
79 Ibid s 6(1).
80 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 203.
81 Ibid pt 13 div 5.

acquired in the course of carrying out his or her duties, except in the performance of those duties.[82]

Oversight and accountability mechanisms

37.53 The Integrity Commissioner is required to give an annual report to the Minister for Home Affairs to be presented to the Parliament.[83] The Commissioner also is required to give investigation and inquiry reports to the Minister if public hearings were held in the course of an investigation.[84] The Minister must remove certain information—such as information that may endanger a person's life or physical safety or prejudice certain proceedings—before tabling such a report in Parliament.[85] The Integrity Commissioner also may give special reports to the Minister on the operations of his or her office for presentation to the Parliament.[86]

37.54 The Integrity Commissioner must notify the Minister of any issue concerning the corrupt conduct of a current or former ACLEI staff member, and staff are under a similar obligation to report corruption by the Integrity Commissioner.[87] Any member of the public also may refer to the Minister an allegation of corruption in the ACLEI or provide the Minister with information relating to such an allegation.[88] The Minister may refer the issue to the Integrity Commissioner for investigation, or authorise a special investigator—who has the same investigative and reporting powers that would be available to the ACLEI—to investigate the issue.[89]

37.55 After the first three years of operation, the Minister must cause an independent review of the ACLEI Act to be undertaken, unless a parliamentary committee or the Parliament Joint Committee on the ACLEI has started or completed a review of the operation of the Act before the end of the three-year period.[90]

37.56 The LEIC Act established a Parliamentary Joint Committee on the ACLEI.[91] The functions of the Committee are to

- monitor and review the Integrity Commissioner's performance of his or her functions;
- examine the annual reports and special reports of the Integrity Commissioner;

82 Ibid s 207.
83 Ibid s 201.
84 Ibid s 203(1).
85 Ibid s 203(2).
86 Ibid s 204.
87 Ibid s 153.
88 Ibid s 154.
89 Ibid s 154.
90 Ibid s 223A.
91 Ibid pt 14.

- examine and report on trends and changes in corruption issues and recommend changes to the functions, powers and procedures of the Integrity Commissioner; and

- conduct an inquiry into any question in connection with the Committee's duties that is referred by either House of Parliament.[92]

37.57 In addition, the Commonwealth Ombudsman has the power to investigate complaints against the ACLEI that relate to administrative matters.[93] The Integrity Commissioner also is subject to regular inspection and monitoring by the Commonwealth Ombudsman in relation to the exercise of his or her powers to carry out controlled operations under Part IAB of the *Crimes Act*, use surveillance devices under the *Surveillance Devices Act*, and undertake telecommunications interception and access stored communications under the *Telecommunications (Interception) Act*.[94]

37.58 State and territory jurisdictions that have anti-corruption bodies commonly provide for their partial exemption from the operation of privacy laws or standards. In New South Wales, the Independent Commission Against Corruption and the Police Integrity Commission are not required to comply with the information protection principles under the *Privacy and Personal Information Protection Act 1998* (NSW), except in connection with the exercise of their administrative and educative functions.[95] In Victoria, the Office of Police Integrity falls within the definition of 'law enforcement agency' and therefore is not required to comply with a number of Information Privacy Principles under the *Information Privacy Act 2000* (Vic).[96] Similarly, the Queensland Crime and Misconduct Commission is defined as a 'law enforcement agency' under the *Information Standard No 42* (Qld) and therefore is exempt from compliance with five of the 11 Information Privacy Principles under the Standard.[97]

---

92 Ibid s 215.

93 *Ombudsman Act 1976* (Cth) s 5.

94 *Crimes Act 1914* (Cth) s 15UB; *Surveillance Devices Act 2004* (Cth) s 55; *Telecommunications (Interception) Act 1979* (Cth) ss 83, 152.

95 The exemption also applies to the inspectors and staff of both the Independent Commission Against Corruption and the Police Integrity Commission: *Privacy and Personal Information Protection Act 1998* (NSW) s 27.

96 *Information Privacy Act 2000* (Vic) s 3 (definition of 'law enforcement agency'), 13.

97 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.2.1], [7] (definition of 'law enforcement agency'). The Standard also does not cover certain personal information that may be handled by the Crime and Misconduct Commission, including personal information: (a) arising out of or in connection with certain controlled and covert operations and activities of the Crime and Misconduct Commission; (b) arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* (Cth); (c) about a witness who is included in a witness protection program or subject to certain witness protection arrangements; (d) arising out of a complaint made under pt 7 of the *Police Service Administration Act 1990* (Qld); and (e) contained in a public interest disclosure within the meaning of the *Whistleblowers Protection Act 1994* (Qld), or that has been collected during an investigation arising out of a public interest disclosure: Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.2.2].

37.59 Under the Information Privacy Bill 2007 (WA), the Corruption and Crime Commission in Western Australia generally will be exempt from compliance with privacy legislation.[98]

Discussion Paper proposals

37.60 In DP 72, the ALRC expressed the preliminary view that government agencies that perform an oversight role, such as the Integrity Commissioner, serve an important public interest in ensuring that government agencies that are vested with coercive powers are monitored and held accountable. This public interest should, however, be balanced with the need to protect the privacy of personal information. The ALRC noted the OPC's submission on the Issues Paper, *Review of Privacy* (IP 31) that it would be desirable for the ACLEI to develop information-handling guidelines, or alternatively, for the *Privacy Act* to apply to the administrative operations of the ACLEI.[99] The ALRC proposed that the Integrity Commissioner should be partially exempt from the operation of the *Privacy Act* except in respect of the non-administrative operations of his or her office.[100] In addition, the ALRC proposed that the Integrity Commissioner should be subject to information-handling guidelines in respect of the non-administrative operations of his or her office.[101]

Submissions and consultations

37.61 Some stakeholders supported the proposal to extend the coverage of the *Privacy Act* to the Integrity Commissioner in respect of the administrative operations of his or her office.[102] The Cyberspace Law and Policy Centre submitted that no agency should be completely exempt from compliance with fundamental human rights and administrative law principles. It argued that agencies like the ACLEI should be required to justify any exemption from both the *Privacy Act* and the related provisions of the FOI Act. It also suggested that, where an exemption is justified, information-handling guidelines should be developed and published in consultation with the OPC.[103]

37.62 In contrast, the ACLEI submitted that a complete exemption from the operation of the *Privacy Act* is necessary for its effective operation. It argued that the exemption is necessary for the purposes of:

- ensuring the ACLEI's inquisitorial power, which may be used to gather intelligence about a corruption issue, is not subject to unintended fetter;

---

98 Information Privacy Bill 2007 (WA) sch 2.
99 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
100 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 34–3.
101 Ibid, Proposal 34–4.
102 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; P Youngman, *Submission PR 394*, 7 December 2007.
103 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

- restricting possibilities for counter-surveillance tactics to be used against the ACLEI that might otherwise frustrate the ACLEI's operations, having particular regard to the law enforcement skills, knowledge, and access to information of those who may be subject to corruption inquiries; and
- ensuring there are no impediments to the voluntary flow of information from any source that might identify corruption.[104]

37.63 The ACLEI submitted that its information handling already is sufficiently regulated by provisions under the LEIC Act, including provisions concerning its objects, functions and confidentiality requirements. The ACLEI argued that its exemption poses a very small risk to the privacy of individuals, because it collects little personal information of an administrative nature in practice and that information would be limited in scope. The ACLEI stated that it only has 10 investigative, legal, policy and corporate staff and therefore its information-handling practices in respect of its administrative operations would affect few people. In addition, the ACLEI submitted that:

> The Integrity Commissioner recognises the importance of appropriately handling personal information. As far as possible, the Information Privacy Principles and the Privacy Commissioner's Guidelines form an important part of ACLEI's management of personal information.[105]

37.64 The ACLEI suggested that it was more comparable to the ACC than to oversight bodies, in that both the ACLEI and the ACC use similar investigative powers and methods, as well as inquisitorial powers, in the performance of their functions. The ACLEI submitted that, while it has an oversight role, there are four critical differences between the ACLEI and other oversight bodies such as the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman, which relate to:

- the Integrity Commissioner's coercive inquisitorial power which may be exercised in a public or a private hearing;
- the ACLEI's law enforcement function and intrusive powers;
- the special nature of those who may fall subject to the ACLEI's investigations—law enforcement officers engaged in corruption, but who are also skilled in countersurveillance and other law enforcement methodologies; and
- a focus on achieving prosecutions and disciplinary outcomes, rather than remedies for complainants.[106]

37.65 In addition, the ACLEI submitted that a partial exemption that requires it to comply with the *Privacy Act* in respect of its administrative operations would be an impractical and disproportionate response to the issue of privacy. The ACLEI argued that, due to its investigative and intelligence-gathering methodologies, it is not always

---

104 Australian Commission for Law Enforcement Integrity, *Submission PR 449*, 11 December 2007.
105 Ibid.
106 Ibid.

possible to distinguish between its administrative and non-administrative operations—especially since its covert operations relate to personnel and financial management that should not be subject to normal constraints on use and disclosure.

> While this problem may affect other law enforcement agencies that use covert methodologies, including paid informants, in the case of the ACLEI the risk of compromise is increased because of the counter-surveillance knowledge of targets of the ACLEI's investigations, who are themselves trained in similar methodologies.[107]

37.66 The ACLEI also argued that the coverage of its administrative operations by the *Privacy Act* would pose a risk to its effective operation and the personal safety of some of its employees and those who give assistance to it. ACLEI stated that, since it may become a target for infiltration and compromise, administrative records concerning current or former employees should not be made available to the employee and their use or disclosure should not be constrained.[108]

37.67 Moreover, ACLEI suggested that, where federal, state and international agencies are not compelled to provide information about corruption to the ACLEI, the narrowing of its privacy exemption may have an adverse impact on the willingness of these agencies to volunteer information.[109]

37.68 On the other hand, the ACLEI accepted the ALRC's proposal that the Integrity Commissioner, in consultation with the OPC, develop and publish information-handling guidelines for the ACLEI.[110] This proposal also was supported by other stakeholders.[111]

ALRC's view

37.69 Due to the serious threat to society posed by corruption, the ACLEI is given coercive information-gathering powers and inquisitorial powers in carrying out its functions. While the ACLEI is not subject to the *Privacy Act*, it is subject to confidentiality provisions under the LEIC Act and oversight by the Parliamentary Joint Committee on the ACLEI and the Commonwealth Ombudsman. It also has reporting obligations to the AGD and, in the event of a suggestion of corruption, the Minister for Home Affairs.

---

107 Ibid.

108 Ibid.

109 Ibid.

110 The ACLEI advised that it has commenced discussion with the OPC on the development of appropriate guidelines, and that the Integrity Commissioner intended to refer monitoring of the guidelines to the ACLEI's Internal Audit Committee: Ibid.

111 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; Australian Commission for Law Enforcement Integrity, *Submission PR 449*, 11 December 2007. The National Archives of Australia submitted that it should be included in any discussions in the development of information-handling guidelines that apply to the Integrity Commissioner: National Archives of Australia, *Submission PR 414*, 7 December 2007.

37.70 Like the ACC, therefore, the ACLEI is subject to a separate system of oversight and accountability. This separate system accommodates the tension between oversight requirements and the need to avoid disclosure of the ACLEI's sensitive operations. In these circumstances, the OPC may not be the appropriate body to deal with complaints against the ACLEI. In addition, the ALRC accepts the submission by the ACLEI that a partial exemption that applies to the Integrity Commissioner in respect of the administrative operations of his or her office may be impractical, for example, matters relating to ACLEI's covert operations concern law enforcement officers, which includes ACLEI's officers, it may not always be possible to distinguish between the administrative and non-administrative operations of the ACLEI.

37.71 In light of these considerations, the Integrity Commissioner and the staff members of ACLEI should continue to be exempt from the operation of the *Privacy Act*. They should be required, however, to comply with information-handling guidelines which should be developed and published in consultation with the OPC. The development of such guidelines will ensure that personal information is handled appropriately, without compromising the ACLEI's operations. The guidelines should reflect the model UPPs to the maximum extent possible. In line with the ALRC's recommendation concerning the ACC, such guidelines also should address the conditions to be imposed on the recipients of personal information disclosed by the Integrity Commissioner or the ACLEI in relation to the further handling of that information. This will ensure that the continuity of privacy protection of personal information held on the ACLEI's records is preserved. Further, the information-handling guidelines should address whether there is a need to establish a suitable complaint-handling mechanism for privacy-related complaints that do not fall within the jurisdiction of the Commonwealth Ombudsman.

37.72 The ALRC notes that the development and publication of such information-handling guidelines received support from both the OPC and the ACLEI. As mentioned above, the ACLEI advised that it has commenced discussion with the OPC concerning the development of such guidelines, which are to be monitored by its Internal Audit Committee.[112] In addition to the ACLEI's Internal Audit Committee, compliance with the information-handling guidelines also should be monitored by the Parliamentary Joint Committee on the ACLEI.

Recommendation 37–2 (a) The Integrity Commissioner, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity (ACLEI). The information-handling guidelines should address the conditions to be imposed on the recipients of personal information disclosed by the Integrity Commissioner or the ACLEI in relation to the further handling of that information.

112 Australian Commission for Law Enforcement Integrity, *Submission PR 449*, 11 December 2007.

(b) The Internal Audit Committee of the ACLEI and the Parliamentary Joint Committee on the ACLEI should monitor compliance by the Integrity Commissioner and the ACLEI with the information-handling guidelines.

Other agencies with law enforcement functions

Background

37.73 With the exception of the ACC, the Integrity Commissioner and staff members of ACLEI, law enforcement agencies and other agencies with law enforcement functions are covered by the *Privacy Act* and therefore must comply with the IPPs. Section 6(1) of the *Privacy Act* relevantly provides that, with certain exceptions, an agency includes 'a body … established or appointed for a public purpose by or under a Commonwealth enactment'. Accordingly, agencies with law enforcement functions, such as ASIC and the Australian Customs Service, fall within the definition of 'agency' under the *Privacy Act*.[113] In addition, the AFP is included expressly within the definition of 'agency' under the Act.[114]

37.74 Given the need to balance the interests of privacy with the public interest in law enforcement and the regulatory objectives of government,[115] however, the *Privacy Act* provides for specific exceptions to a number of the IPPs. Under IPPs 10 and 11, agencies are permitted to use or disclose personal information in certain circumstances. In the context of law enforcement, two exceptions are of particular relevance. IPPs 10.1(c) and 11.1(e) authorise the use or disclosure of personal information if it is 'reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue'.[116] IPPs 10.1(c) and 11.1(d) also allow the use or disclosure of personal information by agencies if the use or disclosure is 'required or authorised by or under law'.[117]

---

113 ASIC was established by s 7 of the *Australian Securities and Investments Commission Act 1989* (Cth) (superseded) to regulate companies and financial services, and promote investor, creditor and consumer protection under the *Corporations Act 2001* (Cth), the *Australian Securities and Investments Commission Act 2001* (Cth) and other legislation: *Australian Securities and Investments Commission Act 2001* (Cth) ss 11, 12A; Australian Securities and Investments Commission, *ASIC Annual Report 2006–07* (2007), 32. ASIC continues in existence by virtue of s 261 of the *Australian Securities and Investments Commission Act 2001* (Cth). The Australian Customs Service was established by s 4 of the *Customs Administration Act 1985* (Cth) to manage the security and integrity of Australia's border, facilitate the movement of legitimate travellers and goods across the border, and collect border-related duties and taxes under the *Customs Act 1901* (Cth), the *Customs Tariff Act 1995* (Cth) and other legislation: Australian Customs Service, *Annual Report 2006–07* (2007), 5.

114 *Privacy Act 1988* (Cth) s 6(1).

115 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001), 1.

116 Where personal information is used or disclosed for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the agency must include in the record containing that information a note of that use or disclosure: *Privacy Act 1988* (Cth) s 14, IPPs 10.2, 11.2.

117 See also Ch 16.

37.75 In addition, some IPPs have been interpreted to include law enforcement considerations within their terms. For example, IPP 2 provides that an agency collecting personal information about an individual is to 'take such steps (if any) as are, in the circumstances, reasonable' to ensure that the individual concerned generally is aware of the purpose for which the information is being collected and other matters. In the context of the investigation of unlawful activities, 'reasonable steps' have been interpreted as including taking no step at all, in circumstances where a suspect should not be alerted to the fact of the collection of personal information about him or her.[118]

37.76 Furthermore, under IPPs 5.2, 6 and 7, if an agency is required or authorised under an applicable federal law to do so, it may refuse to provide an individual with information about what personal information is held about him or her, access to a record or the right to correct or amend documents containing personal information about the individual held by the agency. For example, s 37 of the FOI Act provides that an agency does not have to provide access to, or allow correction of, documents if the disclosure of the document would, or could reasonably be expected to:

- prejudice the conduct of an investigation or the enforcement or proper administration of the law in a particular instance;
- disclose the existence or identity of a confidential source of information in relation to the enforcement or administration of the law;
- endanger the life or physical safety of any person;
- prejudice the fair trial or impartial adjudication of a particular case;
- disclose lawful methods for dealing with breaches or evasions of the law that would, or would be reasonably likely to, prejudice the effectiveness of those methods; or
- prejudice the maintenance or enforcement of lawful methods for the protection of public safety.

37.77 In addition to exceptions to the IPPs that apply to law enforcement agencies, the *Privacy Act* also contains exceptions to the National Privacy Principles (NPPs) that allow organisations to cooperate lawfully with agencies performing law enforcement functions. These exceptions may allow an organisation to use, disclose, or deny access to, personal information for certain law enforcement or regulatory purposes.[119]

---

118 Office of the Federal Privacy Commissioner, *Taking Reasonable Steps to Make Individuals Aware that Personal Information about Them is Being Collected*, Information Sheet 18 (2003), 4–5.

119 *Privacy Act 1988* (Cth) s 6; sch 3, NPPs 2.1, 6.1.

37.78 NPP 2.1 provides that an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection except in specified circumstances. These include the use and disclosure of personal information where it is: for the purposes of reporting or investigating unlawful activity; required or authorised by or under law; and reasonably necessary for a range of activities carried out by, or on behalf of, an enforcement body.[120] The range of activities include:

> (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
>
> (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
>
> (iii) the protection of the public revenue;
>
> (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
>
> (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.[121]

37.79 NPP 6.1 provides further that an organisation must, on request by an individual, provide the individual with access to personal information it holds about him or her, subject to certain exceptions. These exceptions include where: providing access would be unlawful; denying access is required or authorised by or under law; providing access would be likely to prejudice an investigation of possible unlawful activity; providing access would be likely to prejudice certain law enforcement activities; and an enforcement body performing a lawful security function asks the organisation not to provide access to the information, on the basis that providing access would be likely to cause damage to the security of Australia.[122]

37.80 The *Privacy Act*, therefore, in conjunction with other federal legislation (such as the FOI Act), provides a number of exceptions to the privacy principles that allow agencies to carry out their law enforcement activities. One issue raised in this Inquiry is whether these exceptions should instead be provided for by way of an exemption.

37.81 In Chapter 33, a distinction is drawn between exemptions and partial exemptions to the requirements set out in the *Privacy Act*, and exceptions to the privacy principles. An *exemption* applies where a specified entity or a class of entity is not required to comply with any of the requirements in the *Privacy Act*. A *partial exemption* applies where a specified entity or a class of entity is required to comply with either: some, but not all, of the provisions of the *Privacy Act*; or some or all of the provisions of the *Privacy Act*, but only in relation to certain of its activities. An *exception*, as applied to the privacy principles, applies where a requirement in the

---

120 Ibid sch 3, NPP 2.1(f)–(h).
121 Ibid sch 3, NPP 2.1(h).
122 Ibid sch 3, NPP 6.1(g)–(k).

privacy principles does not apply to any entity in a specified situation or in respect of certain conduct.

International privacy instruments

37.82 International privacy instruments commonly provide for exceptions to the principles that apply to criminal investigations. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines) recognise that member countries may apply the OECD Guidelines differently to different kinds of personal data or in different contexts, such as criminal investigations.[123] The OECD Guidelines also state that criminal investigative activities are one area where, for practical or policy reasons, an individual's knowledge or consent cannot be considered necessary for the collection of his or her personal data.[124]

37.83 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament contains exceptions to the privacy principles, including for the processing of data necessary for the prevention, investigation, detection and prosecution of criminal offences,[125] and concerning public security, state security and the activities of the state in areas of criminal law.[126] Article 13 of the EU Directive provides that member states may provide for exceptions from specified data processing principles if they are necessary to safeguard public security or for the prevention, investigation, detection and prosecution of criminal offences. The principles from which such exceptions are permitted include those relating to: data quality; information to be given to the individual concerned; an individual's right of access to data; and the publicising of data processing operations.[127]

37.84 Like the EU Directive, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework states that it is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy interests.[128]

Other jurisdictions

37.85 Criminal investigation also is a common exception to data protection principles in overseas jurisdictions, such as the United Kingdom, New Zealand and Hong Kong.

---

123 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Memorandum, [47].

124 Ibid, Memorandum, [47].

125 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 13(1)(d).

126 Ibid, art 3(2).

127 Ibid, art 13. See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recitals 16, 43.

128 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13]. See also Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [31].

Under the *Data Protection Act 1998* (UK), certain data protection principles do not apply if the application of those principles would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature. The principles that do not apply include: further processing of personal data should be compatible with the original purpose of collection; fair processing by notification to the individual concerned; an individual's rights of access and correction; data quality; data retention; and an individual's right to prevent processing.[129]

37.86 The *Privacy Act 1993* (NZ) provides for exceptions to some of the information privacy principles contained in that Act, where non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including: the prevention, detection, investigation, prosecution, and punishment of offences; and the enforcement of a law imposing a pecuniary penalty.[130] The relevant principles include those concerning collection of personal data directly from the individual concerned, notification to individuals about certain matters, and use and disclosure of personal information.

37.87 Hong Kong privacy legislation provides for exceptions to the use and access principles contained in that legislation, where compliance with those principles is likely to prejudice: the prevention or detection of crime; apprehension, prosecution or detention of offenders; and prevention, preclusion or remedying of other unlawful conduct.[131]

37.88 In contrast, some Australian states provide for law enforcement activities in their privacy legislation by way of exemptions rather than exceptions. In New South Wales, for example, there are detailed exemptions for law enforcement bodies, such as the state and territory police force, the New South Wales Crime Commission, the AFP, the ACC, and the state and territory directors of public prosecutions.[132] Similarly, in Victoria, a law enforcement agency is exempt from compliance with certain privacy principles under the *Information Privacy Act 2000* (Vic) in specified circumstances.[133]

Discussion Paper question

37.89 In DP 72, the ALRC recognised the need to consider 'how the protection of personal and sensitive information is best balanced with the broad and unpredictable nature of policing activities'. The AFP observed that, although law enforcement functions and requirements can be understood to be within the terms of the IPPs, there is no explicit recognition of operational policing in the privacy principles concerning collection (IPPs 1–3), and access and correction (IPPs 6 and 7). It suggested that an

---

129 *Data Protection Act 1998* (UK) s 29.
130 *Privacy Act 1993* (NZ) ss 6 (Principles 2, 3, 10, 11), 27.
131 *Personal Data (Privacy) Ordinance* (Hong Kong) s 58.
132 *Privacy and Personal Information Protection Act 1998* (NSW) s 3(1).
133 Examples of law enforcement agencies include the state or territory police force, the AFP and the ACC: *Information Privacy Act 2000* (Vic) s 3.

option for reform would be to extend the exceptions to the IPPs in line with the approach under the EU Directive, and the New South Wales and Victorian privacy legislation. The AFP submitted that this approach would be a more transparent way for the *Privacy Act* to set out the range of circumstances in which police can collect, analyse, and disclose personal and sensitive information. It stated that this also would clarify the interaction between the *Privacy Act*, and the secrecy and disclosure provisions in other legislation.[134]

37.90 The ALRC considered that, before it could make a proposal, it would require submissions from a larger number of stakeholders. The ALRC therefore asked whether the *Privacy Act* should be amended to set out, in the form of an exemption, the range of circumstances in which agencies that perform law enforcement functions are not required to comply with specific privacy principles.[135]

Submissions and consultations

37.91 Some stakeholders opposed the idea of setting out law enforcement functions in the form of an exemption from the *Privacy Act*, rather than exceptions to the privacy principles.[136] The OPC submitted that exceptions to the privacy principles provide more flexibility and consistency than exemptions.

> One of the major advantages of prescribing exceptions to the principles of the *Privacy Act*, rather than exemptions, is that they could apply to a range of entities when performing certain types of functions … In contrast, given their absolute nature, exemptions may not be sufficiently flexible to accommodate the variety of activities for which an agency may handle personal information. The Office notes that only a portion of an agency's normal activities may clearly merit being placed outside the general scope of the principles.[137]

37.92 Given the wide range of entities that fall within the definition of an 'enforcement body' in the *Privacy Act*, the OPC submitted that 'it is unclear how select activities of this diverse group could be adequately captured by an exemption provision without affecting privacy protections relating to other functions'. In addition, the OPC suggested that:

> by exempting a limited number of enforcement agencies when performing particular functions, there is a risk that other agencies that occasionally perform similar enforcement functions would have to meet different requirements for handling the personal information. This would create additional inconsistencies and promote regulatory complexity and uncertainty … exceptions are arguably better placed to deal with the handling of personal information by a broader range of entities in specific contexts.[138]

---

134 Australian Federal Police, *Submission PR 186,* 9 February 2007.

135 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 34–1.

136 Public Interest Advocacy Centre, *Submission PR 548,* 26 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.

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

138 Ibid.

37.93 In addition, the OPC submitted that information-handling practices required under the *Privacy Act* improve data quality and promote better decision making, especially in the law enforcement context. It noted that decisions based on poor information can have an adverse impact on individuals and the reputation of enforcement agencies, which could in turn undermine community trust and confidence in these agencies and the administration of the law. It was of the view that:

> the *Privacy Act* includes the right balance of requirements and necessary exceptions for the efficient and effective operation of enforcement agencies including intelligence, investigations and public safety functions.[139]

37.94 While PIAC accepted that there is a conflict between law enforcement work and compliance with the privacy principles in some circumstances, it was of the view that a general exemption for agencies that perform law enforcement functions 'may lead to a perception that these agencies somehow stand outside privacy law'.[140]

37.95 Both the OPC and PIAC also noted that there already are a number of exceptions to the privacy principles that take into account law enforcement considerations, which were reflected in the UPPs.[141]

37.96 Law enforcement and regulatory bodies, on the other hand, supported setting out law enforcement functions as exemptions from the operation of the *Privacy Act*.[142] The AFP supported a general exemption that allows it to perform all of its functions under the *Australian Federal Police Act 1979* (Cth).[143] The Australian Taxation Office (ATO) submitted that both law enforcement and regulatory bodies should be provided with an exemption from compliance with specific privacy principles in a range of circumstances. The ATO argued that its functions in intelligence gathering (such as activities to identify tax avoidance arrangements and promoters), and in safeguarding the financial interests of the state, are recognised as acceptable bases for an exemption from the operation of privacy laws.[144]

37.97 Victoria Police submitted that exemptions for law enforcement agencies are essential in the areas of law enforcement, intelligence, and community policing functions and activities. It suggested that, given the changing nature of policing, community policing functions should be included in a law enforcement exemption.[145]

37.98 It also was submitted that some law enforcement agencies perform both law enforcement and regulatory functions, and that any distinction made in the *Privacy Act*

---

139 Ibid.
140 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
141 Ibid; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
142 Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Victoria Police, *Submission PR 523*, 21 December 2007.
143 Australian Federal Police, *Submission PR 545*, 24 December 2007.
144 Australian Taxation Office, *Submission PR 515*, 21 December 2007.
145 Victoria Police, *Submission PR 523*, 21 December 2007.

between law enforcement and regulatory agencies should indicate clearly that some agencies perform both types of functions.[146]

37.99 The Australian Privacy Foundation submitted that law enforcement functions should be set out as exemptions, provided that such exemptions can be justified through a process of public consultation. It suggested that, while some information may need to be withheld from the public consultation process on security grounds, a wholly secret process would not be justified.[147]

37.100 The United Nations Youth Association, the Flinders Law Students' Association and the Adelaide University Law Students' Society submitted that privacy laws should not prevent the collection and storage of personal information of convicted offenders, on the basis of an online survey they conducted. The online survey of 332 respondents—the majority of whom were young people undertaking tertiary studies—showed that 73% of respondents believed that new laws allowing the permanent retention of DNA samples from suspects, convicted criminals and prisoners were justified.[148] The student and youth bodies suggested that the result of this survey was 'broadly consistent with widespread trust in government', and that the respondents generally seemed 'unconcerned by mass accruement of information by government'.[149]

Application of the proposed UPPs to law enforcement agencies

37.101 Law enforcement and regulatory bodies raised concerns about the application of some of the proposed UPPs to their activities.[150] In relation to the proposed 'Anonymity and Pseudonymity' principle, it was submitted that some law enforcement agencies may require individuals to provide accurate identification. It was argued that a legislative right for an individual to deal with an agency or organisation anonymously or pseudonymously may interfere substantially with the law enforcement agency's functions.[151]

37.102 Particular concerns were raised about the application of the proposed 'Collection' principle to the collection of sensitive information by law enforcement agencies, including that:

- law enforcement agencies often collect sensitive information from third parties and therefore should not be required to collect personal information about an individual only from that individual;[152]

---

146 Confidential, *Submission PR 448*, 11 December 2007.
147 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
148 Approximately 15% of respondents disagreed, while 11% of respondents did not know whether the new laws were justified: United Nations Youth Association, Flinders University Students' Association and Adelaide University Law Students' Society, *Submission PR 557*, 7 January 2007.
149 Ibid.
150 See, eg, Victoria Police, *Submission PR 523*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.
151 Confidential, *Submission PR 448*, 11 December 2007.
152 Ibid.

- it would be impractical and undesirable for law enforcement agencies either to seek the consent of individuals to collect sensitive information, or to prove in every case that the collection is necessary to prevent or lessen a serious threat to the life or health of an individual;[153] and

- in some circumstances, it may be difficult for a law enforcement agency to make a case that the collection of sensitive information was 'required or specifically authorised by or under law', as some legislation may not specifically authorise certain investigative and intelligence-gathering activities that are a part of the agency's law enforcement functions.[154]

37.103 Some stakeholders submitted that the application of the proposed 'Notification' principle to law enforcement agencies would be problematic, because notifying individuals in relation to personal information collected through intelligence-gathering activities of such agencies would alert the individuals to the fact that they are under investigation.[155] The ATO submitted that a requirement to notify individuals also would be inappropriate where the information used for prosecution or other civil action by law enforcement agencies was initially collected for a different purpose; and when the ATO receives anonymous information about an individual taxpayer that may identify potential tax avoidance and promotional activities.[156] The ATO considered that the requirement to notify individuals in these circumstances would: impose a significant administrative burden on the ATO; reduce the likelihood of detection of tax avoidance arrangements and tax avoidance scheme promoters by putting them on notice of the ATO's intent; and increase ill-feeling within the community as taxpayers attempt to identify anonymous informants.[157]

37.104 Victoria Police submitted that law enforcement agencies should not be required to comply with the proposed 'Data Quality' principle. It argued that, since law enforcement agencies often collect information in anticipation that it may be relevant, the requirement that law enforcement agencies collect only relevant information would hinder their law enforcement capabilities and intelligence capacity.[158]

37.105 One stakeholder submitted that the proposed 'Identifiers' principle—which prevents an agency or organisation from adopting an identifier of an individual except in prescribed circumstances—would affect the ability of law enforcement agencies to cooperate on information exchange across government.[159] Concern also was raised as to whether the proposed 'Cross-border Data Flows' principle would prevent the

---

153 Ibid.
154 Victoria Police, *Submission PR 523*, 21 December 2007; Confidential, *Submission PR 448*, 11 December 2007.
155 Australian Taxation Office, *Submission PR 515*, 21 December 2007; Confidential, *Submission PR 448*, 11 December 2007.
156 Australian Taxation Office, *Submission PR 515*, 21 December 2007.
157 Ibid.
158 Victoria Police, *Submission PR 523*, 21 December 2007.
159 Confidential, *Submission PR 448*, 11 December 2007.

transfer of personal information by law enforcement agencies to recipients in other countries where this is required or authorised by legislation.[160]

ALRC's view

37.106 Agencies with law enforcement functions should continue to operate within the privacy principles and the applicable exceptions to those principles. The model UPPs are sufficiently flexible to accommodate the functions and operations of agencies with law enforcement and regulatory functions. Exceptions to the UPPs have the advantage of flexibility as they can apply to a range of entities when performing specific functions, and they also are capable of adapting to changing circumstances—for example, when agencies are given or stripped of law enforcement functions—without requiring any amendment to privacy legislation.

37.107 In addition, it is doubtful whether an exhaustive list of exempt activities in relation to each of these agencies would provide more clarity than the exceptions to the UPPs. Currently, there are a number of agencies that perform a diverse range of law enforcement functions—for example, the AFP, the Australian Customs Service, ASIC, the ATO and Centrelink. An exhaustive list of the numerous law enforcement and regulatory functions that these agencies perform in the *Privacy Act* would render the Act unnecessarily detailed and unwieldy.

37.108 The ALRC notes the submissions by law enforcement and regulatory bodies that considers that the application of the UPPs, as proposed in DP 72, could be problematic. The ALRC has taken these concerns into account and modified the model UPPs where appropriate. For example, the ALRC has removed the proposed requirement that the collection of sensitive information must be 'specifically authorised by of under law' to take into account the fact that some legislation may authorise, but not specifically, the collection of sensitive information.[161] In Chapter 16, the ALRC notes that case law on 'authorised by or under law' shows that authorisation requires permission and not merely an absence of prohibition. The ALRC accepts the submissions by agencies that the inclusion of the term 'specifically authorise' in the *Privacy Act* arguably may prevent them from relying on implied authorisations to carry out their statutory functions and exercise their powers. The ALRC therefore expresses the view that the term 'specifically authorised' should not be adopted in the *Privacy Act*.

37.109 Further, the ALRC recommends in Chapter 30 that the 'Identifiers' principle should apply only to organisations. In Chapter 31, the ALRC recommends that the 'Cross-border Data Flows' principle should provide that, where an agency or organisation transfers personal information to a recipient outside of Australia and an external territory, it remains accountable for that information unless, among other things, it is required or authorised by or under law to make the transfer.

---

160 Ibid.
161 See Ch 22.

37.110 Other concerns raised by law enforcement agencies relate to the interpretation of what is 'practicable', 'reasonable' or 'relevant' in the circumstances. These are issues that can be addressed by guidance issued by the OPC. One concern raised was that the requirement to give an individual the option of dealing with a law enforcement agency anonymously or pseudonymously could interfere substantially with the agency's law enforcement functions. The ALRC notes, however, that under the 'Anonymity and Pseudonymity' principle, agencies and organisations only are required to provide that option where it is lawful and practicable. It is clear that there will be circumstances where a law enforcement agency would not be required to give individuals that option, on the basis that it would not be lawful or practicable to do so.[162] The ALRC therefore does not share the concern that the 'Anonymity and Pseudonymity' principle would interfere with the functions of law enforcement agencies.

37.111 Another concern raised by stakeholders is that the requirements under the 'Notification' principle may: conflict with the intelligence-gathering process of law enforcement agencies; alert an individual to the fact that he or she is under investigation; or identify an informant. The 'Notification' principle, however, only requires that an agency or organisation take reasonable steps to notify an individual or ensure that the individual is aware of certain matters. While taking reasonable steps has been interpreted to include taking no steps in appropriate circumstances,[163] the ALRC has further clarified the requirement by amending the 'Notification' principle so that an agency or organisation only is required to 'take such steps, if any, as are reasonable in the circumstances' to notify.[164] It is clearly not reasonable to notify an individual of the fact of collection when a law enforcement agency is collecting intelligence on an individual who is suspected of committing an offence, or where to do so would identify an informant during the investigative process. A law enforcement agency, therefore, would not be required to take any steps to notify the individual in those circumstances.

37.112 The ALRC also notes the concern that requiring agencies to collect only relevant information under the 'Data Quality' principle may hinder the activities of law enforcement agencies. In this regard, the ALRC notes that IPP 3 also requires an agency to take reasonable steps to ensure that the information it collects is relevant to the purpose of collection. The OPC has advised that, where personal information is generally related to their intelligence-gathering purposes, law enforcement agencies may collect such information even if they do not have an immediate use for it or do not know exactly what the information will be used for—provided that they have good grounds for believing that this kind of information would be of assistance.[165]

---

162 See Ch 20.

163 Office of the Federal Privacy Commissioner, *Taking Reasonable Steps to Make Individuals Aware that Personal Information about Them is Being Collected*, Information Sheet 18 (2003), 5.

164 See Ch 23.

165 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 24, 28.

37.113 The ALRC notes that the OPC has issued both general and specific guidance on the application of the *Privacy Act* in the context of unlawful activities and law enforcement.[166] In addition, elsewhere in this Report, the ALRC makes a number of recommendations concerning the development and publication of guidance by the OPC to assist agencies and organisations in complying with the model UPPs.[167] Guidance issued by the OPC should take into account the application of the model UPPs to law enforcement activities and address the concerns raised by law enforcement and regulatory bodies.

166 See Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001); Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 13, 14, 23, 24, 28; Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998); 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).

167 See Recs 16–2, 19–1, 20–2, 21–2, 21–4, 23–3, 25–3, 28–5, 29–9, 31–7.

38. Other Public Sector Exemptions

Contents

Introduction

38.1 The preceding chapters in this Part examine the exemption of a number of agencies from the operation of the *Privacy Act 1988* (Cth), including: defence and intelligence agencies; federal courts; certain agencies listed in the *Freedom of Information Act 1982* (Cth) (FOI Act); and agencies with law enforcement functions. This chapter discusses the exemption of a number of other agencies from the operation of the Act—namely, Royal Commissions, the commission of inquiry into the 2007 equine influenza outbreak, state and territory authorities, and prescribed state and territory instrumentalities.

Commissions of inquiry

Royal Commissions

38.2 A federal Royal Commission is a government inquiry established by the Governor-General pursuant to the *Royal Commissions Act 1902* (Cth). The *Royal Commissions Act* allows the Governor-General, by Letters Patent, to

> issue such commissions, directed to such person or persons, as he thinks fit, requiring or authorizing [those persons] to make inquiry into and report upon any matter specified in the Letters Patent, and which relates to or is connected with the peace, order and good government of the Commonwealth, or any public purpose or any power of the Commonwealth.[1]

38.3 Royal Commissions are established on an ad hoc basis to inquire into matters of public interest. Their purpose is usually to ascertain factual circumstances and make recommendations.[2] There have been a number of high profile federal Royal Commissions, including those into the Australian Wheat Board, HIH Insurance, the building and construction industry, and Aboriginal deaths in custody.[3]

38.4 A federal Royal Commission has coercive information-gathering powers. For example, it has the power to summon a witness to give evidence or produce documents.[4] Further, the *Royal Commissions Act* creates a number of statutory offences for certain types of conduct. For example, it is an offence to fail to attend or produce documents to a Royal Commission; or to conceal, mutilate or destroy any document or thing that is likely to be required in evidence before a Royal Commission.[5]

38.5 A federal Royal Commission may order that evidence be taken in private. It may also limit or prohibit the publication of certain material, such as the evidence given before it or information that might enable a witness to be identified.[6] In addition, regulations may be made for the custody, use or disclosure of records of a Royal Commission that are no longer required for its purposes.[7]

38.6 A federal Royal Commission exercises powers that usually are exercised by courts. Nevertheless,

> the function which is primarily distinctive of judicial power—the power to decide or determine—is absent. The commission can neither decide nor determine anything and nothing that it does can in any way affect the legal position of any person. Its powers and functions are not judicial.[8]

---

1 *Royal Commissions Act 1902* (Cth) s 1A

2 T Cole, *Report of the Inquiry into Certain Australian Companies in relation to the UN Oil-for-Food Programme* (2006), [7.65].

3 See Ibid; N Owen, *Report of the HIH Royal Commission* (2003); T Cole, *Royal Commission into the Building and Construction Industry* (2003); E Johnstone, *Royal Commission into Aboriginal Deaths in Custody* (1991).

4 *Royal Commissions Act 1902* (Cth) s 2.

5 Ibid ss 3, 6K.

6 Ibid s 6D (2)–(5).

7 Ibid s 9. Custody of Royal Commission records may only be given to certain persons or bodies, such as a federal, state or territory attorney-general, the Director of Public Prosecutions, specified law enforcement and regulatory agencies, the Secretary of the Department of the Prime Minister and Cabinet, and the National Archives of Australia: *Royal Commissions Act 1902* (Cth) s 9(3).

8 *Lockwood v Commonwealth* (1954) 90 CLR 177, 181.

38.7 A federal Royal Commission is an 'agency' for the purposes of the *Privacy Act*. Its acts and practices, however, are not acts and practices to which the Act applies.[9] Accordingly, federal Royal Commissions are not regulated by the *Privacy Act*.

38.8 It has been argued that Royal Commissions have greater powers than courts to force revelations and even confessions, because they do not presume either innocence or guilt and do not make determinations. Accordingly, there is a risk that individuals appearing before Royal Commissions may be forced to make embarrassing revelations and face exposure, humiliation and adverse publicity without regard for the appropriate balance between privacy and open justice.[10]

The commission of inquiry into the equine influenza outbreak

38.9 On 2 September 2007, the then Prime Minister and the then Minister for Agriculture, Fisheries and Forestry announced the establishment of an inquiry into the outbreak of equine influenza in Australia in August 2007.[11] The *Quarantine Amendment (Commission of Inquiry) Act 2007* (Cth) amended the *Quarantine Act 1908* (Cth) to provide for the appointment of a person to conduct a commission of inquiry into the equine influenza outbreak and related quarantine requirements and practices.[12]

38.10 The Commission was vested with most of the powers of a Royal Commission.[13] In addition, people engaged to assist the Commission were entitled to exercise powers under the *Quarantine Act* in certain circumstances.[14]

38.11 The *Quarantine Amendment (Commission of Inquiry) Act* also amended the *Privacy Act* to provide that the acts and practices of the Commission were not acts and practices to which the *Privacy Act* applied.[15] Thus, the Commission was exempt from the operation of the Act. The amendment was made to ensure that the records of the commission of inquiry were 'managed in accordance with existing procedures for royal commissions'.[16] The Commission has concluded its inquiry and presented its report to the Hon Tony Bourke MP, Minister for Agriculture, Fisheries and Forestry.[17]

---

9 *Privacy Act 1988* (Cth) s 7(1)(a)(v).

10 M Rayner, 'Commissions and Omissions' (1996) 6(10) *Eureka Street* 14.

11 J Howard (Prime Minister) and P McGauran (Minister for Agriculture, Fisheries and Forestry), *Joint Press Conference*, 2 September 2007.

12 *Quarantine Amendment (Commission of Inquiry) Act 2007* (Cth) sch 1, cl 5.

13 *Quarantine Act 1908* (Cth) s 66AZE.

14 Ibid s 66AZC, pt VIA.

15 *Privacy Act 1988* (Cth) ss 6, 7(1)(vi).

16 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 September 2007, 1 (P McGauran—Minister for Agriculture, Fisheries and Forestry), 2.

17 T Burke (Minister for Agriculture, Fisheries and Forestry), 'Government Receives Equine Influenza Inquiry Report' (Press Release, 24 April 2008).

38.12 In New Zealand, Royal Commissions and other commissions of inquiry are completely exempt from the operation of the *Privacy Act 1993* (NZ).[18]

Submissions and consultations

38.13 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether federal Royal Commissions should be wholly or partially exempt from the operation of the *Privacy Act*.[19] The Office of the Privacy Commissioner (OPC) submitted that, although the *Privacy Act* may not be the appropriate instrument to deal with concerns regarding the operation of Royal Commissions, 'attention should be given to developing information handling standards for Royal Commissions that promote respect for privacy'. The OPC suggested that the matter be referred to the Attorney-General of Australia.[20]

38.14 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the Attorney-General's Department, in consultation with the OPC, should develop and publish information-handling guidelines for Royal Commissions to assist in ensuring that the personal information they handle is protected adequately.[21] There was some support for this proposal.[22] The Cyberspace Law and Policy Centre, however, submitted that no agency should be completely exempt from the need to comply with fundamental human rights and administrative law principles. It argued that agencies such as Royal Commissions should be required to justify any exemption from the operation of the *Privacy Act* and related provisions in the FOI Act. It submitted that, where an exemption is justified, information-handling guidelines should be developed and published in consultation with the OPC.[23]

38.15 The National Archives of Australia (National Archives) submitted that it should be included in any discussions about the development of information-handling guidelines for Royal Commissions.[24]

ALRC's view

38.16 Royal Commissions serve the important function of inquiring into matters of public interest. Central to the performance of this function is the ability of Royal Commissions to obtain information that may be unavailable by other means of investigation or inquiry. Although they do not exercise judicial power, they are given powers that usually are exercised by courts.

---

18 *Privacy Act 1993* (NZ) s 2(1) (definition of 'agency').
19 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.
20 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
21 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 34–1.
22 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.
23 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
24 National Archives of Australia, *Submission PR 414*, 7 December 2007.

38.17 The exemption of Royal Commissions from the *Privacy Act* is warranted. To ensure that Royal Commissions handle personal information appropriately, information-handling guidelines that apply to Royal Commissions should be developed by the Department of the Prime Minister and Cabinet, which now has responsibility for administering the *Privacy Act*. The guidelines should be developed in consultation with the OPC, which should, in turn, consult with all relevant stakeholders, such as the National Archives, about the content of the guidelines.

38.18 The Commission of Inquiry into the equine influenza outbreak was established after the publication of DP 72 and has now concluded. The ALRC notes, however, that the same rationale for exempting Royal Commissions from the *Privacy Act* is likely to apply to commissions of inquiry that are not established under the *Royal Commissions Act*. Where such commissions of inquiry are exempt from the operation of the *Privacy Act*, they should adhere to the information-handling guidelines that are to be developed for Royal Commissions.

Recommendation 38–1 The Department of the Prime Minister and Cabinet, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for Royal Commissions.

State and territory authorities

38.19 State and territory authorities are not agencies or organisations for the purposes of the *Privacy Act*.[25] Accordingly, they are exempt from the operation of the Act unless they are brought into the regime by regulation.[26] Generally, state and territory authorities are people or bodies that are part of a state or territory public sector, such as state and territory ministers and government departments; local governments; and bodies and tribunals established for public purposes under state and territory laws.[27]

38.20 State and territory bodies that are incorporated companies, societies or associations, however, are considered 'organisations' for the purposes of the Act.[28] They can be prescribed out of the coverage of the Act, but only upon the request of the relevant state or territory and only after the Minister responsible for administering the *Privacy Act* has considered a number of issues outlined in the Act.[29]

---

25 *Privacy Act 1988* (Cth) ss 6(1), 6C.
26 Ibid s 6F.
27 Ibid s 6C(3); Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 2.
28 *Privacy Act 1988* (Cth) s 6C(1), (3)(c)(i).
29 Ibid s 6C(4); Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 2.

38.21 Some state and territory authorities are required by other federal legislation to comply with the *Privacy Act*. For example, public and private sector higher education providers are required by the *Higher Education Support Act 2003* (Cth) to comply with the Information Privacy Principles (IPPs) when handling the personal information of students obtained for the provision of financial assistance to students.[30]

38.22 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that the reason for the exemption of state and territory authorities from the *Privacy Act* was that the acts and practices of state and territory public sector agencies were for the states and territories to regulate.[31]

38.23 From 21 December 2001 to 31 January 2005, 16% of all the complaints about the National Privacy Principles (NPPs) closed by the OPC because they were outside its jurisdiction concerned the exemption for state and local governments.[32] In 2004–05, the OPC received 2,469 enquiries concerning exemptions, of which 32% related to state or local government bodies not covered by the *Privacy Act*.[33]

Prescribed state and territory instrumentalities

38.24 A state or territory instrumentality is an 'organisation' for the purposes of the *Privacy Act*. Accordingly, a state or territory instrumentality is subject to the private sector provisions of the Act. The Governor-General may, however, make regulations under s 6C(4) of the *Privacy Act* to prevent a state or territory instrumentality from being treated as an organisation.

38.25 Section 6C(4) provides that, before any such regulations are made, the Minister must be satisfied that the state or territory in question has requested that the instrumentality be prescribed as falling outside the definition of organisation for the purposes of the Act. Further, the Minister must consider certain factors when making such regulations. These are:

- whether treating the instrumentality as an organisation for the purposes of the *Privacy Act* adversely affects the government of the state or territory;
- the desirability of regulating the handling of personal information by the instrumentality under the *Privacy Act*; and

---

30 *Higher Education Support Act 2003* (Cth) s 19.60.

31 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [73].

32 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

33 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 38. No statistics on the number of inquiries concerning exempt state and local bodies were reported for 2005–06 or 2006–07: see Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006); Office of the Victorian Privacy Commissioner, *Annual Report 2006–07* (2007).

- whether a state or territory law regulates the handling of personal information by the instrumentality to a standard that is at least equivalent to the standard that would apply to the instrumentality under the *Privacy Act*.

38.26 The Minister also must consult with the Privacy Commissioner about these factors.[34] At present, no state or territory instrumentalities have been prescribed.

38.27 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that:

> One of the purposes of [sub-clause 6C(4)] is to recognise that Commonwealth regulation of a State or Territory instrumentality (for example a Corporations Law company, society or association) that performs core government functions is inappropriate, if such regulation would curtail the capacity of the State or Territory to function as a government.[35]

State and territory government business enterprises

38.28 A number of state and territory authorities are government business enterprises (GBEs). GBEs provide a range of services, including communications, transport, employment and health services. The three characteristics that identify GBEs are:

> the Government controls the body; the body is principally engaged in commercial activities; and the body has a legal personality separate to a department of government.[36]

38.29 A state or territory GBE may be a body corporate established by legislation for a public purpose (state-owned or statutory corporations), or a company established under corporations law in which a state or territory government has a controlling interest.

38.30 Currently, there is inconsistent coverage of state and territory statutory corporations under state and territory privacy laws. For example, statutory corporations are covered by privacy legislation in Victoria but not in New South Wales.[37] In Tasmania, GBEs are covered by privacy legislation.[38] The exemption for statutory

---

34 *Privacy Act 1988* (Cth) s 6C(4)(c).

35 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [74].

36 Administrative Review Council, *Report to the Minister of Justice: Government Business Enterprises and Commonwealth Administrative Law*, Report 38 (1995), 7.

37 The *Information Privacy Act 2000* (Vic) applies to 'public sector agency', ie, a public service body or a public entity within the meaning of the *Public Administration Act 2004* (Vic): *Information Privacy Act 2000* (Vic) ss 3, 9(1)(c). Under the *Public Administration Act*, public entities include bodies that are established by or under an Act (other than a private Act) or the Corporations Act: *Public Administration Act 2004* (Vic) s 5. In New South Wales privacy legislation, the definition of 'public sector agency' expressly excludes 'a state owned corporation': *Privacy and Personal Information Protection Act 1998* (NSW) s 3.

38 Under the *Personal Information Protection Act 2004* (Tas) a public sector body includes a GBE under the *Government Business Enterprises Act 1995* (Tas): *Personal Information Protection Act 2004* (Tas) s 3.

corporations in New South Wales was originally justified on the basis that statutory corporations should not be put at a competitive disadvantage with the private sector. The then Attorney General of New South Wales, the Hon Jeff Shaw MLC, stated that:

> When the Act evolves to include coverage of the private sector, State-owned corporations will be similarly covered by the information and privacy principles of the legislation. The Government intends to address this issue in detail following the March 1999 election.[39]

38.31 New South Wales legislation has not yet been amended to cover statutory corporations.

Opt-in provision

38.32 Under s 6F of the *Privacy Act*, state and territory governments may request that certain state and territory authorities or instrumentalities be treated as organisations under the Act. One of the purposes of this opt-in provision

> is to allow statutory corporations whose activities are predominantly commercial, to 'opt-in' to the private sector privacy regime where the State (or Territory) and Minister (in consultation with the Privacy Commissioner) consider that it is appropriate to do so.[40]

38.33 At present, only four state-owned entities have been brought into the federal privacy regime by regulation—Country Energy, EnergyAustralia, Integral Energy Australia and Australian Inland Energy Water Infrastructure.[41]

Should state and territory authorities be exempt from the operation of the Act?

38.34 The report of the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* noted that there was concern that the exemption of state and territory authorities from the operation of the *Privacy Act* represented a significant gap in the Act's coverage.[42]

38.35 In IP 31, the ALRC asked whether state and territory authorities should be exempt from the privacy principles in the *Privacy Act*.[43] The ALRC also asked whether, in addition to the energy distributors owned by the New South Wales

---

39 New South Wales, *Parliamentary Debates*, Legislative Council, 25 November 1998, 10592 (J Shaw—Attorney General).

40 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [96].

41 *Privacy (Private Sector) Regulations 2001* (Cth) reg 3A. Australian Inland Energy Water Infrastructure was subsequently dissolved in July 2005: *Energy Services Corporation (Dissolution of Australian Inland Energy Water Infrastructure) Regulation 2005* (NSW).

42 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.38].

43 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–4.

Government (which are the only state authorities prescribed under the *Privacy (Private Sector) Regulations 2001* (Cth)), there were any other state or territory authorities that should be covered by the privacy principles in the *Privacy Act*.[44]

State and territory authorities generally

38.36 Some stakeholders were of the view that state and territory authorities should be exempt from the Act.[45] For example, the Office of the Information Commissioner (Northern Territory) submitted that it is the responsibility of the state and territory governments to ensure that the privacy of personal information handled by state and territory authorities is protected.[46] The Victorian Office of the Health Services Commissioner stated that:

> Although it is unfortunate that certain state and territory statutory bodies fall outside both the federal and the state privacy regimes … this is not a sufficient reason for the Federal Government to attempt to regulate state and territory public sector agencies.[47]

38.37 Others submitted that certain state and territory authorities should continue to be exempt from the operation of the *Privacy Act*.[48] The New South Wales Guardianship Tribunal submitted that state and territory guardianship tribunals should remain exempt.[49] The Australian Guardianship and Administration Committee submitted that public trustees should be exempt 'from appropriate provisions of the *Privacy Act* … where the Public Trustee is seeking information about a person, from either the private or public sector, in the ordinary course of the Public Trustee's business as trustee'.[50]

38.38 Other stakeholders considered that state and territory authorities should not be exempt from the *Privacy Act*.[51] For instance, the Insurance Council of Australia submitted that state and territory authorities should not be exempt as this creates the potential for conflict between federal and state and territory laws.[52]

---

44 Ibid, Question 5–5.

45 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

46 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

47 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

48 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007; Australian Guardianship and Administration Committee, *Submission PR 129*, 17 January 2007.

49 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007.

50 Australian Guardianship and Administration Committee, *Submission PR 129*, 17 January 2007.

51 Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007.

52 Insurance Council of Australia, *Submission PR 110*, 15 January 2007.

38.39 Some stakeholders submitted that state and territory authorities should be exempt to the extent that they are subject to state and territory privacy laws.[53] The Office of the Victorian Privacy Commissioner (OVPC) stated that federal privacy law should not bind state authorities when they are already subject to state privacy laws, because this would result in unnecessary fragmentation and confusion. The OVPC also did not support state referral of power to the Commonwealth

> as it would remove the state's ability to provide enhanced protection and, while dealing with the constitutional impediment, continues to suffer from the problem of how it is to interact with other state based laws (FOI, archives, human rights etc).[54]

38.40 The OVPC, however, was in favour of federal minimum standards that apply to state and territory public sectors.

> Given that not all jurisdictions have privacy laws in place, there is some merit in the proposal to have minimum standards apply to state and territory public sectors which can be 'rolled back' once that jurisdiction enacts privacy legislation that conforms to the specified federal standard—provided that this allowed for better protection to be adopted by the state and territory governments.[55]

38.41 In addition, the OVPC suggested that the opt-in mechanism in s 6F of the *Privacy Act* should remain, because 'while it appears not to have been used, it may be in the future and this type of mechanism maintains control by and independence of the states'.[56]

38.42 Some stakeholders expressed concern that some state-owned statutory corporations are excluded from both the state and the federal privacy regimes.[57] In addition, some stakeholders noted that the question of the exemption of state and territory authorities from the operation of the *Privacy Act* would fall away if a uniform privacy scheme were adopted.[58] One stakeholder submitted that state and territory agencies should be exempt only on a case-by-case basis.[59]

38.43 It was also suggested that the following state and territory bodies should be regulated by the *Privacy Act*:

---

53 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

54 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

55 Ibid.

56 Ibid.

57 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; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006.

58 Queensland Government, *Submission PR 242*, 15 March 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

59 K Pospisek, *Submission PR 104*, 15 January 2007.

- bodies established by administrative arrangements, including on a cooperative basis between jurisdictions; [60]

- universities established under state or territory legislation;[61] and

- federally funded state entities, such as hospitals, research institutes, universities, schools, environment management agencies and road authorities.[62]

Government business enterprises

38.44 Some stakeholders were of the view that government businesses that compete with private sector organisations should be subject to the *Privacy Act*.[63] In its submission, the OPC stated that

> the acts and practices of state and territory bodies that are responsible for policy development and implementation, and for the making of laws, should generally be subject to the oversight of the respective Parliament, and thus ultimately accountable to the electorate of that jurisdiction. This includes Ministers and departments of state in those jurisdictions and bodies, as well as bodies established for a public purpose by or under a law of that state or territory.[64]

38.45 The OPC submitted, however, that state-owned statutory corporations that function as government businesses should be covered by the *Privacy Act*, because not all states and territories have enacted privacy legislation, and the lack of privacy protection for personal information handled by these statutory corporations may be inconsistent with community expectations. It also submitted that 'applying privacy regulation to state and territory statutory corporations is likely to be consistent with the principle of competitive neutrality'.[65] On this basis, the OPC suggested that:

- the Australian Government should work with all states and territories to implement privacy regulation that is consistent with the *Privacy Act* or adopt the *Privacy Act* as model legislation;

---

60 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

61 Ibid; D Antulov, *Submission PR 14,* 28 May 2006.

62 I Turnbull, *Submission PR 82,* 12 January 2007.

63 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; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

64 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

65 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See National Competition Council, *Compendium of National Competition Policy Agreements* (1998), cl 3.

- the *Privacy Act* should apply to all incorporated bodies, including state and territory statutory corporations, except where there is equivalent privacy legislation in the relevant jurisdiction; and

- where it is considered necessary that state and territory incorporated bodies be exempted from coverage of the *Privacy Act* on public interest grounds, that consideration be given to applying a provision such as s 6C(4) to give effect to the exemption.[66]

38.46 Professor Graham Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that:

> There is no reason why State or Territory business enterprises should have an arguable commercial advantage over private sector organisations because they can avoid the costs of compliance with privacy laws. On the other hand, there is no reason why the Commonwealth should monopolise power to establish appropriate privacy standards. Consistency in privacy standards across Australia is desirable, but that is a separate issue. The best balance is struck simply by ensuring that some enforceable privacy standard applies …
>
> The law should make provision for coverage of any state or territory authorities 'by agreement' (effected through Regulations) to cover the increasing number of 'hybrid' organisations involved in the delivery of public services and to ensure no organisation can 'fall between the gaps'.[67]

Options for reform

38.47 In DP 72, the ALRC noted that the exemption of state and territory authorities from the operation of the *Privacy Act* represented a significant gap in privacy regulation in Australia, and expressed the view that state-owned statutory corporations that compete with organisations should not have a competitive advantage over organisations.[68]

38.48 The ALRC considered that one option for reform would be to require state and territory authorities to comply with the *Privacy Act* unless they were covered by a state or territory law that was 'substantially similar' to the Act. In Canada, the Governor in Council may,

> if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.[69]

---

66 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

67 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

68 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [34.111]–[34.112].

69 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 26(2)(b).

38.49 The Privacy Commissioner of Canada has advised that, in assessing whether provincial legislation is 'substantially similar' to the federal legislation, the Commissioner would

> interpret substantially similar as equal or superior to the [*Personal Information Protection and Electronic Documents Act*] in the degree and quality of privacy protection provided. The federal law is the threshold or floor. A provincial privacy law must be at least as good, or it is not substantially similar.[70]

38.50 Another option would be to be to require state and territory authorities to comply with the *Privacy Act* unless the Privacy Commissioner determines that a particular state or territory authority should be exempt from compliance with the Act.

38.51 The Privacy Commissioner currently performs a similar function in relation to privacy codes. Under the *Privacy Act*, the Privacy Commissioner currently has the power to approve privacy codes.[71] An organisation that is bound by a privacy code is not required to comply with the NPPs.[72] Section 18BB of the *Privacy Act* provides that the Privacy Commissioner must be satisfied of a number of matters before he or she approves a privacy code. In particular, s 18BB(2)(a) provides that the Privacy Commissioner must be satisfied that 'the code incorporates all the National Privacy Principles or sets out obligations that, overall, are at least the equivalent of all the obligations set out in those Principles'.

38.52 The OPC's *Guidelines on Privacy Code Development* provide guidance on how the Privacy Commissioner assesses whether the condition in s 18BB(2)(a) is met.

> In deciding if this condition has been met, the Commissioner requires code proponents to include a statement of claims detailing:
>
> i) how the obligations under the code differ from the obligations under the [NPPs];
>
> ii) the rationale for the change to any obligation provided in the NPPs; and
>
> iii) how, in the opinion of the code proponent, the obligations set out in the code are at least equivalent of all the obligations set out in the NPPs.[73]

The Discussion Paper proposals

38.53 In DP 72, the ALRC proposed that the states and territories enact legislation applying the proposed Unified Privacy Principles (UPPs) and the proposed *Privacy (Health Information) Regulations* to state and territory agencies.[74] The ALRC noted,

---

70 Privacy Commissioner of Canada, *Report to Parliament Concerning Substantially Similar Legislation* (2002), 2.

71 *Privacy Act 1988* (Cth) pt IIIAA. Privacy codes are discussed in Ch 48.

72 Ibid s 16A.

73 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001), 30.

74 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–4.

however, that the implementation of such a scheme would take time.[75] The ALRC therefore proposed that, before the enactment of similar legislation in the states and territories, the *Privacy Act* should be amended to apply to all state and territory incorporated bodies, including statutory corporations, except where they are covered by state or territory privacy law setting out obligations that, overall, are at least the equivalent of the relevant obligations in the *Privacy Act*.[76]

38.54 In deciding the approach for determining whether a state or territory has equivalent privacy law, the ALRC expressed a preference for it to be modelled on s 18BB(2)(a) of the *Privacy Act*, on the basis that the Privacy Commissioner already has experience in assessing equivalence under this provision.

38.55 In addition, the ALRC considered that the *Privacy Act* should provide a mechanism for regulations to be made to exclude certain state and territory bodies from the coverage of the Act on public interest grounds.[77] The ALRC expressed the view that this mechanism should be modelled on s 6C(4) of the *Privacy Act*, which lists the criteria for excluding a state or territory instrumentality from the coverage of the Act.[78]

Submissions and consultations

38.56 A number of stakeholders supported the ALRC's proposed approach.[79] Privacy NSW supported the proposal because state-owned corporations in New South Wales are not subject to either federal or state privacy legislation.

> Given that some of these corporations are utility providers and as such hold large amounts of high value identity information about NSW customers there is a compelling need to make them subject to privacy regulation.[80]

38.57 The Public Interest Advocacy Centre (PIAC) observed that the proposal would fill the current gap in the coverage of state-owned statutory corporations until states and territories enact legislation applying the UPPs to state and territory agencies. PIAC also supported the proposal to empower the Governor-General to make regulations to exempt state and territory incorporated bodies on public interest grounds, provided that there was 'a mechanism for making proposed exemptions public and allowing privacy advocates and consumer groups an opportunity to make submissions'.[81]

---

75 Ibid, [34.113].
76 Ibid, Proposal 34–5(a).
77 Ibid, Proposal 34–5(b).
78 Ibid, Proposal 34–6.
79 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 Direct Marketing Association, *Submission PR 543*, 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; Privacy NSW, *Submission PR 468*, 14 December 2007.
80 Privacy NSW, *Submission PR 468*, 14 December 2007.
81 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

38.58 The Cancer Council Australia and the Clinical Oncological Society of Australia supported the proposed approach, on the basis that it

> would facilitate national uniformity and consistency in the management of health information and the enabling of federal law to override state or territory laws in relation to health data, where clearly in the public interest in terms of individual or community health outcomes.[82]

38.59 The Queensland Government noted that government-owned corporations in Queensland are currently covered the *Privacy Act* and stated that it had 'no objection to the continuation of the situation'. It noted further that it is currently converting all statutory government-owned corporations into company form, which would bring them within the coverage of the *Privacy Act*. The Queensland Government indicated, however, that it would not support extending the coverage of the *Privacy Act* to other statutory bodies, on the basis that this would create a situation where those bodies would have to comply with two sets of privacy obligations. Further, this approach 'would also impinge on the independence of the states and territories to determine how best to carry on the business of the state or territory'.[83]

38.60 The Government of South Australia did not support the proposal to apply the *Privacy Act* to all state and territory bodies. It was concerned that if it did not enact privacy legislation applying the UPPs and the proposed *Privacy (Health Information) Regulations*, its state-owned incorporated bodies may have to comply with both the *Privacy Act* and the Information Privacy Principles under *PC012—Information Privacy Principles Instruction*.

> This would also mean there would be effectively two reporting and complaints mechanisms applying to State owned incorporated bodies. It would seem unnecessary to have this provision when the [PC012] IPPs already provide an adequate level of privacy protection.[84]

ALRC's view

38.61 The exemption of state and territory authorities from the operation of the *Privacy Act* means that only those state and territory authorities that are subject to state and territory privacy laws are covered by privacy regulation. Accordingly, this exemption represents a gap in privacy regulation in Australia in those jurisdictions that have no privacy regulation or where that regulation does not extend to state and territory authorities.

---

82 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007.

83 Queensland Government, *Submission PR 490*, 19 December 2007.

84 Government of South Australia, *Submission PR 565*, 29 January 2008.

38.62 In Chapter 3, the ALRC recommends that the Australian Government and state and territory governments develop and adopt an intergovernmental agreement in relation to the handling of personal information. This agreement should establish an intergovernmental cooperative scheme whereby the states and territories enact legislation regulating the handling of personal information in the state and territory public sectors. This legislation should apply the model UPPs, any regulations modifying the application of the UPPs, and relevant definitions used in the *Privacy Act*. Further, it should contain certain minimum provisions, including provisions regulating state and territory incorporated bodies (including statutory corporations).[85] The enactment of such legislation will resolve issues concerning the inadequate or inconsistent regulation of state and territory incorporated bodies.

38.63 The implementation of the recommended intergovernmental scheme is likely to take time. The ALRC is no longer of the view, however, that in the interim the *Privacy Act* should be amended to apply to all state and territory incorporated bodies that are not covered by obligations under a state or territory law that are the equivalent of the relevant obligations in the *Privacy Act*. The ALRC notes the concerns raised by some stakeholders that this could create further inconsistency and fragmentation in privacy regulation in Australia. The ALRC agrees that it is not desirable to implement a scheme that may require some state or territory incorporated bodies to comply with both state or territory privacy obligations and obligations imposed by the *Privacy Act.*

38.64 In Chapter 3, the ALRC recommends that the Australian Government initiate a review in five years from the commencement of the amended *Privacy Act* to consider whether the recommended intergovernmental cooperative scheme has been effective in achieving national consistency. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy to cover the field, including in the state and territory public sectors.[86] The nature and extent of the regulation of state and territory incorporated bodies should be considered during this review.

38.65 Finally, the ALRC agrees that the 'opt-in' mechanism contained in s 6F of the *Privacy Act* is a useful mechanism to bring state and territory bodies under the operation of the *Privacy Act* and should be retained in the Act.

---

85 Rec 3–4.
86 Rec 3–6.

39. Small Business Exemption

Contents

Introduction

39.1 Generally speaking, small businesses—namely, those with an annual turnover of $3 million or less—are exempt from the operation of the *Privacy Act 1988* (Cth).[1] This exemption is commonly known as the 'small business exemption'. It has been estimated that up to 94% of Australian businesses may fall under this exemption.[2] The

1 *Privacy Act 1988* (Cth) s 6C.

2 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.20]. The

small business exemption has been scrutinised by four separate inquiries since 2000, when the *Privacy Act* was extended to the private sector.[3] In this chapter, the ALRC examines the competing arguments on reform of the exemption and concludes that the small business exemption should be removed.

39.2 Having regard to the need to minimise unnecessary compliance costs on small businesses, however, the ALRC recommends that, before the removal of the exemption, the Office of the Privacy Commissioner (OPC) should provide substantial support and assistance to small businesses to assist them in understanding and fulfilling their obligations under the *Privacy Act*. Such assistance would include a national hotline for small businesses, educational materials on the requirements under the Act, templates for Privacy Policies and educational programs targeted at small businesses.

Background

Current law

39.3 Under s 6C of the *Privacy Act*, a small business operator is excluded specifically from the definition of 'organisation' and generally is exempt from the operation of the Act. A 'small business operator' is an individual, body corporate, partnership, unincorporated association or trust that carries on one or more small businesses, and does not carry on a business that is not a small business.[4]

39.4 A 'small business' is a business that had an annual turnover of $3 million or less in the previous financial year (or in the current financial year if it is a new business).[5] 'Small businesses' can include non-profit bodies and unincorporated associations,[6] even though the ordinary meaning of the term 'business' may not include such bodies.

---

estimate was based on Australian Bureau of Statistics, *Business Growth and Performance Survey, Financial Year 1997/1998* (1999), which has been discontinued since then.

3 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000); Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

4 *Privacy Act 1988* (Cth) s 6D(3).

5 Ibid s 6D(1). The annual turnover of a business for a financial year includes the proceeds of sales of goods and/or services; commission income; repair and service income; rent, leasing and hiring income; government bounties and subsidies; interest, royalties and dividends; and other operating income earned in the year in the course of business: *Privacy Act 1988* (Cth) s 6DA. It does not include assets held by small businesses, capital gains or proceeds of capital sales: Office of the Privacy Commissioner, *A Privacy Checklist for Small Business (Updated with Minor Amendments 27 November 2007)* (2007), 4.

6 Office of the Privacy Commissioner, *A Snapshot of the Privacy Act for Small Business (Updated with Minor Amendments 27 November 2007)* (2007), 1.

39.5 There are a number of conditions that qualify the exemption for small businesses. A small business may be captured by the *Privacy Act* if it:

- provides a health service and holds any health information except in an employee record;[7]
- collects personal information about another individual from, or discloses such information to, anyone else for benefit, service or advantage (unless it always has the consent of the individuals concerned, or only does so when required or authorised by or under legislation);[8]
- is or was contracted to provide services to the Australian Government or its agencies;
- is related to a larger business;
- is a 'reporting entity'—that is, a person who provides a 'designated service'—within the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act);[9]
- is prescribed by regulation;[10] or
- elects to 'opt in' to be treated as if it were an 'organisation' within the meaning of the *Privacy Act*.[11]

39.6 The minister responsible for administering the *Privacy Act* also may prescribe that certain small businesses or their activities be subject to the Act. The minister may do so if it is in the public interest and after consultation with the Privacy Commissioner.[12] This provision was intended to enable otherwise exempt small

---

7 Examples of health service providers holding health information which is not contained in an employee record include medical practices, pharmacies and health clubs: Australian Government Attorney-General's Department, *Small Business* (2000) <www.ag.gov.au> at 23 April 2008. An 'employee record' is defined to mean a record of personal information relating to the employment of the employee: *Privacy Act 1988* (Cth) s 6(1).

8 *Privacy Act 1988* (Cth) s 6D(7), (8). See also Office of the Privacy Commissioner, *What Does 'Trading in Personal Information' Mean?* <www.privacy.gov.au/faqs/sbf/q2.html> at 23 April 2008.

9 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5. 'Designated services' include a number of specified financial, bullion trading or gambling services, as well as services prescribed by regulation: *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 6.

10 Regulation 3AA of the *Privacy (Private Sector) Regulations 2001* (Cth) provides that small business operators that operate residential tenancy databases, or those that collect, maintain, use and disclose personal information in connection with such databases, are to be treated as 'organisations' within the meaning of the *Privacy Act 1988* (Cth).

11 *Privacy Act 1988* (Cth) ss 6D(4), (9), 6E, 6EA.

12 Ibid s 6E(4). Currently the minister with responsibility for administering the *Privacy Act* is the Cabinet Secretary.

businesses to be brought within the federal privacy scheme if their activities are found to constitute a particular risk to individual privacy.[13]

39.7 The OPC keeps a register of those businesses that choose to 'opt in'. Currently there are 184 small businesses that have opted to be covered by the *Privacy Act*.[14]

39.8 When the private sector amendments were enacted, small businesses were exempted on the basis that many do not pose a high risk to privacy.[15] The Australian Government took the view that many small businesses do not have significant holdings of personal information, and those that may have customer records do not sell or otherwise deal with customer information in a systematic way that poses a high risk to their customer's privacy.[16]

39.9 It also was the policy of the Australian Government to minimise compliance costs on small businesses.[17] The specified conditions that qualify the application of the small business exemption were intended to acknowledge that some personal information and some activities pose a higher risk to privacy than others, and that small businesses within these categories (such as health service providers) ought to be covered by the Act.[18]

39.10 For the period from 21 December 2001 to 31 January 2005, 20% of all the National Privacy Principles (NPPs) complaints closed by the OPC as outside of its jurisdiction concerned the small business exemption.[19] In 2005–06, the OPC received 2,000 enquiries concerning exemptions, of which 21% related to the small business exemption.[20]

39.11 There are no provisions for an exemption for small businesses in any of the major international privacy instruments—namely, the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD), the European Union's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) or the Asia-Pacific Economic

---

13 Australian Government Attorney-General's Department, *Small Business* (2000) <www.ag.gov.au> at 23 April 2008.

14 Office of the Privacy Commissioner, *Opting-In to Privacy Act Coverage* <www.privacy.gov.au/business/register> at 23 April 2008.

15 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 6.

16 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General), 22370–22371.

17 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 6.

18 Ibid, 6.

19 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

20 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 27. The OPC's most recent annual report does not contain statistics on enquiries concerning exemptions: see Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007).

Cooperation (APEC) Privacy Framework.[21] Further, there are no similar exemptions in comparable jurisdictions, such as the United Kingdom, Canada and New Zealand.[22]

Previous inquiries

39.12 The small business exemption was introduced in the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Privacy Amendment (Private Sector) Bill was the subject of two parliamentary committee inquiries—the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry (2000 House of Representatives Committee inquiry)[23] and the Senate Legal and Constitutional Legislation Committee inquiry (2000 Senate Committee inquiry).[24]

39.13 Despite noting a number of criticisms of the small business exemption, the 2000 House of Representatives Committee inquiry took the view that an effective regulatory balance must be achieved in order to avoid overburdening small businesses that pose a low privacy risk, and that this could not be achieved without some form of exemption for small businesses.[25] The 2000 Senate Committee inquiry recommended the retention of the exemption, on the basis that it 'achieve[s] an adequate balance between concerns about the coverage of the exemption and the intention not to impose too great a burden on small businesses'.[26]

39.14 In 2005, both the OPC and the Senate Legal and Constitutional References Committee reviewed the private sector provisions of the *Privacy Act*.[27] Submissions to the review by the OPC of the private sector provisions of the *Privacy Act* (OPC Review) were roughly divided between support for retention of the small business exemption and its repeal.[28] The OPC Review recommended that the Australian Government should retain but modify the small business exemption by amending the *Privacy Act* so that the definition of small business is expressed in terms of the

---

21 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995); Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

22 *Data Protection Act 1998* (UK); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada); *Privacy Act 1993* (NZ).

23 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000).

24 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000).

25 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.16].

26 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.11]–[3.12].

27 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

28 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 180.

Australian Bureau of Statistics (ABS) definition—20 employees or fewer— rather than annual turnover.[29]

39.15 The 2005 Senate Legal and Constitutional References Committee privacy inquiry (Senate Committee privacy inquiry) questioned the need to retain the small business exemption. It considered that privacy rights of individuals should be protected regardless of whether they were dealing with a small business, and that protecting these rights also made commercial sense for all businesses. Given that privacy regimes in overseas jurisdictions have operated effectively without the exemption, and that the existence of the exemption was one of the key outstanding issues preventing recognition of Australian privacy laws under the EU Directive,[30] the inquiry recommended that the small business exemption be removed from the *Privacy Act*.[31]

39.16 The Senate Committee privacy inquiry also recommended that the ALRC investigate possible measures that could assist Australia in achieving European Union (EU) adequacy.[32] The issue of EU adequacy is discussed in detail in Chapter 31. Briefly, the EU Directive restricts the export of personal data from an EU Member State to a recipient country that does not have an 'adequate level of protection'.[33] Australian businesses that wish to trade with EU organisations must have contractual clauses in place to ensure the adequate protection of personal data transferred from the EU.[34] In March 2001, the Article 29 Data Protection Working Party of the European Commission released an opinion expressing concern about the sectors and activities excluded from the protection of the *Privacy Act* and mentioned, in particular, the small business and employee records exemptions.[35]

39.17 The OPC Review noted that negotiations with the European Commission on this issue were continuing, especially in relation to the small business and employee records exemptions,[36] and concluded that, although there was no evidence of a broad business push for EU adequacy, there may be long term benefits for Australia in achieving this status. The OPC Review, therefore, recommended that the Australian

---

29 Ibid, rec 51.

30 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

31 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32]–[7.34], rec 12.

32 Ibid, rec 16. The Australian Government disagreed with this recommendation, on the basis that 'international negotiations are a matter for the Australian Government and negotiations with the European Union are ongoing': 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), 5.

33 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), arts 25, 26.

34 Ibid, art 26(2).

35 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 3.

36 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

Government continue to work with the EU on this issue.[37] The Australian Government agreed with this recommendation.[38]

39.18 In addition, the OPC Review noted that the increasingly global flow of information makes the development of international privacy frameworks important. The OPC also recommended, therefore, that the Australian Government continue to work within APEC to implement the APEC Privacy Framework.[39]

39.19 In its response to the OPC Review and the Senate Committee privacy inquiry, the Australian Government has maintained its support for retaining the small business exemption,[40] stating that:

> the small business exemption strikes an appropriate balance between the risk of privacy breaches and over regulation of small businesses. Removal of the exemption would be inconsistent with the Government's commitment to workplace reform and cutting red tape.[41]

The scope of the exemption

39.20 As noted above, under the *Privacy Act* a 'small business' is a business that has an annual turnover of $3 million or less in the previous financial year (or in the current financial year if it is a new business).[42] There are no recent official data showing the number of small business operators in Australia with an annual turnover of $3 million or less.

39.21 The ABS, however, does publish data on the number of businesses with an annual turnover of less than $2 million. As at June 2007, there were 1,890,213 businesses with an annual turnover of $2 million or less, which represented 94% of all actively trading businesses in Australia.[43] Accordingly, the number of small businesses eligible for the exemption is likely to exceed 1.9 million. This figure, however, does not take into account the fact that not all small businesses qualify for the exemption—for example, those that trade in personal information without the consent of the individuals concerned.

---

37 Ibid, Rec 17.

38 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 4.

39 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 17.

40 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 10.

41 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), 4.

42 *Privacy Act 1988* (Cth) s 6D(1).

43 Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), 20.

39.22 In evidence before the 2000 House of Representatives Committee inquiry, the Department of Employment, Workplace Relations and Small Business stated that:

> given the likelihood of the existence of high privacy risk low staff number businesses in, for example, the personal service sector or the online world, it was decided that an annual turnover figure that would capture the same number of businesses as the ABS measure should be used.[44]

39.23 The Department also advised the inquiry that:

> based on the ABS *Business Growth and Performance Survey 1997–98*, approximately 94% of all Australian businesses fall under the $3 million threshold. The Department also noted that the survey indicated that the 95% of Australian businesses that are small businesses accounted for only 30% of total sales of goods and services. On this basis the Department estimated that the proportion of private sector business activity undertaken by small businesses was around 30%.[45]

39.24 The 2000 House of Representatives Committee inquiry accepted that the setting of any threshold figure would appear arbitrary.[46] It preferred, however, the use of an annual turnover threshold, arguing that the use of employee numbers to define small businesses could have the unintended consequence of exempting high-risk internet-based businesses.[47]

High-risk sectors

39.25 Since the introduction of the private sector provisions of the *Privacy Act*,[48] certain small business operators have been brought under the *Privacy Act* because their activities pose a particularly high risk to privacy. For example, significant privacy concerns about small business operators that operate residential tenancy databases were raised in four separate inquiries between 2000 and 2005.[49] As a result, the *Privacy (Private Sector) Regulations 2001* (Cth) were amended to prescribe as 'organisations' all small business operators that operate residential tenancy databases, as well as those

---

44 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.19] (footnotes omitted).

45 Ibid, [2.20] (footnotes omitted). The Australian Bureau of Statistics, *Business Growth and Performance Survey, Financial Year 1997/1998* (1999) was conducted by the ABS from 1994–95 to 1997–98. It has been discontinued since then.

46 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.22].

47 Ibid, [2.21].

48 *Privacy Amendment (Private Sector) Act 2000* (Cth).

49 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), rec 19; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 9, 15, 16, 52; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32]; Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), 48–50.

that collect, maintain, use and disclose personal information in connection with such databases.[50]

39.26 Other small business operators that have been identified as posing a high risk to privacy, however, have not been brought under the *Privacy Act*. Submissions to the OPC Review and the Senate Committee privacy inquiry identified a number of other small businesses with significant holdings of personal information that carry out some of the most privacy-intrusive activities, including: businesses that operate within the telecommunications industry, such as internet service providers (ISPs); debt collectors; private investigators;[51] and dating agencies.[52]

39.27 In addition, the passage of the *Northern Territory National Emergency Response Act 2007* (Cth) and related legislation to deal with issues of drug abuse and child sexual assault in the Northern Territory has raised concerns among privacy and other human rights advocates about the handling of personal information by exempt small businesses.[53] This is discussed in detail below.

Discussion Paper proposal

39.28 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC considered whether the small business exemption should be removed. The ALRC expressed the preliminary view that the exemption is neither necessary nor justifiable, and that the cost of compliance with the *Privacy Act* alone does not provide a sufficient policy reason to support the exemption. The ALRC noted that privacy legislation in overseas jurisdictions does not contain an equivalent exemption.

39.29 The ALRC stated that the risks to privacy posed by small businesses are determined primarily by the nature of personal information held, the nature of the business, and the way personal information is handled, rather than by size. The ALRC noted that modifying the exemption would not resolve the concerns raised by stakeholders that any definition of 'small business' would be arbitrary and that consumers cannot determine easily whether the exemption applies to a particular

---

50 *Privacy (Private Sector) Amendment Regulations 2007 (No 3)* (Cth). The amendment took effect on 1 December 2007. Privacy issues concerning residential tenancy databases are discussed further in Ch 17.

51 The ALRC notes that the small business exemption generally does not apply to private investigators, as they trade in personal information without the consent of the individuals concerned: see *Privacy Act 1988* (Cth) s 6D(4)(c), (d), (7), (8). Privacy issues relating to private investigators are discussed in detail in Ch 44.

52 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 180; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.48]–[4.49].

53 Office of the Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs, Inquiry into the Northern Territory National Emergency Response Bill 2007 and Related Bills*, 1 August 2007; Office of the Victorian Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Northern Territory National Emergency Response Bill 2007 and Related Bills*, 10 August 2007; Aboriginal and Torres Strait Islander Social Justice Commissioner, *Social Justice Report 2007* (2008), Ch 3.

business. In addition, regulating small businesses in some areas and not others would add to the complexity of the privacy regime, and modifying the application of the privacy principles to small businesses would result in uneven privacy protection. Accordingly, the ALRC proposed that the small business exemption be removed.[54]

Arguments for removing the exemption

39.30 The main arguments for removing the exemption include that:

- there are no appropriate criteria that could exempt only those small businesses that pose a low risk to privacy, because any definition of 'small business' would be arbitrary;
- removing the exemption would reduce inconsistency and fragmentation in privacy regulation;
- removing the exemption would facilitate trade with the EU; and
- some small businesses, especially those in high-risk sectors, handle large amounts of personal information and carry out some of the most privacy-intrusive activities.

The 'small business' criterion

39.31 A large number of stakeholders supported the ALRC's proposal to remove the small business exemption.[55] Some expressed concern at the high percentage of businesses exempted from protecting individuals' personal information.[56] The fact that

---

54 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 35–1.

55 See, eg, 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; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 535*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; Australian Digital Alliance, *Submission PR 422*, 7 December 2007 (endorsed by Australian Library and Information Association, *Submission PR 446*, 10 December 2007); Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

56 Privacy NSW, *Submission PR 468*, 14 December 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

a substantial number of all complaints against organisations closed by the OPC were closed because they fell within the small business exemption was also a cause of concern.[57] The Office of the Victorian Privacy Commissioner (OVPC) stated that:

> About 30% of enquiries to my office result in referrals to the federal Office of the Privacy Commissioner, and the majority of these relate to small businesses which are likely to currently be exempt under the federal Act.[58]

39.32 Some stakeholders submitted that protection of privacy rights should not depend on the size of the business.[59] It was argued that the ability of a business to misuse personal information is not related to its size,[60] and that the consequences of misuse by small businesses could be just as severe as misuse by larger businesses.[61]

39.33 Other stakeholders questioned whether the assumptions that small businesses are unlikely to hold significant amounts of personal information, and that they are unlikely to deal with it inappropriately, were valid.[62] Some small businesses—such as internet businesses—do in fact hold large amounts of personal information.[63] The Australian Communications and Media Authority (ACMA) submitted that:

> The increasing use of technology by small businesses, who may not be experienced in dealing with privacy matters places increasing pressure on the relevance of the small business exemption currently in the Privacy Act.[64]

39.34 There was concern among stakeholders that consumers may not be able to determine with any certainty whether the small business exemption applies to the business they are dealing with,[65] since annual turnover figures are rarely disclosed publicly.[66] National Legal Aid noted that removing the small business exemption

---

57 Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

58 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

59 Ibid; Government of South Australia, *Submission PR 187,* 12 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

60 ACTU, *Submission PR 155,* 31 January 2007.

61 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; ACTU, *Submission PR 155,* 31 January 2007.

62 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

63 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

64 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

65 Government of South Australia, *Submission PR 565,* 29 January 2008; National Legal Aid, *Submission PR 521,* 21 December 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

66 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

> would resolve uncertainties which currently prevent members of the public from exercising their privacy rights or identifying the obligations of organisations [with which] they deal.[67]

39.35 Further, it was submitted that businesses themselves also may be uncertain about whether they are covered by the small business exemption—a problem that may be complicated further by the conditions that qualify the application of the exemption.[68] For example, the Legal Aid Commission of New South Wales noted that the Law Council of Australia was unable to provide clear guidance about whether law firms are covered by the exemption.[69]

39.36 Some stakeholders were concerned that the small business exemption, together with the exemption applying to related bodies corporate, may be used by large organisations to evade their responsibilities under the *Privacy Act* by transferring data-collection activities to a smaller entity within their corporate structure.[70] Another stakeholder submitted that the small business exemption was a barrier to efforts by particular industries to promote public confidence in the handling of personal information by small businesses.[71]

Regulatory inconsistency and fragmentation

39.37 Some stakeholders noted that the small business exemption contributes to the complexity of the privacy regime.[72] The Queensland Government expressed particular concern about the complexity of the exemptions regime in the education sector:

> Non-State schools may or may not be required to comply based on a number of tests, for example annual turnover and the collection of 'health information'. Exempt non-state schools may also choose to 'opt in' to the regime. The three tiered approach that currently operates—determined by the size of the school and the collection of one type of information—can create inconsistencies in the management of personal information in educational contexts.[73]

39.38 National Legal Aid noted that the application of the privacy regime to the provision of legal services was complicated, because some non-government organisations provide government-funded public services and therefore may not

---

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

68 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

69 Ibid.

70 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

71 Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502,* 20 December 2007.

72 Queensland Government, *Submission PR 242,* 15 March 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.

73 Queensland Government, *Submission PR 242,* 15 March 2007.

qualify for the small business exemption. It suggested that coverage of such non-government organisations would avoid this complication.[74]

39.39 Some stakeholders suggested that the small business exemption adversely affects the consistency of privacy regulation across Australia.[75] For example, one individual submitted that the coverage of small businesses by some state privacy legislation, but not the federal *Privacy Act*, caused confusion.

> People could find themselves referred back and forth between the Commonwealth and NSW Privacy Offices if there is any doubt as to the annual turnover of the allegedly offending company.[76]

39.40 The OVPC stated that privacy protection should be consistent and universal across Australia, and that there was no policy justification for completely exempting small businesses from the operation of the *Privacy Act*. The OVPC stated that every organisation should be required to protect the privacy of personal information it has collected, especially where the information is sensitive.[77] National Legal Aid submitted that:

> Uniform coverage means that organisations and individuals can rely on clearly stated privacy obligations when dealing with small businesses and non government organisations, and on forms of alternative dispute resolution under the Privacy Act as a realistic alternative to legal action. Uniform coverage should ease the task of the Privacy Commissioner when providing education and advice.[78]

39.41 The Queensland Government noted that the removal of the small business exemption, together with the proposed removal of the employee records exemption, would fill a gap in coverage and ensure national consistency in the regulation of the private sector. It stated that the two proposals were 'in line with the current examination by [the Standing Committee of Attorneys-General] of workplace privacy, and would answer a number of the issues identified during that process'.[79]

39.42 The Government of South Australia submitted that 'business efficacy is not likely to be enhanced by misuse or careless management of personal information'.[80] It stated that the benefits of removing the exemption would include:

- clarifying consumers' confusion and closing off loopholes under the exemption, thus promoting public confidence in the effectiveness of the privacy regime;

---

74 National Legal Aid, *Submission PR 521,* 21 December 2007.
75 Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502,* 20 December 2007; P Youngman, *Submission PR 394,* 7 December 2007.
76 P Youngman, *Submission PR 394,* 7 December 2007.
77 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.
78 National Legal Aid, *Submission PR 521,* 21 December 2007.
79 Queensland Government, *Submission PR 490,* 19 December 2007.
80 Government of South Australia, *Submission PR 187,* 12 February 2007.

- creating a level playing field for all small businesses, as currently some small businesses are not exempt and others choose to opt in;

- promoting good business management practice and helping to build business reputation; and

- further harmonising the trans-Tasman privacy protection regime.[81]

39.43 Some stakeholders identified other ways to modify the impact of the *Privacy Act* on small businesses. It was suggested, for example, that the removal of the small business exemption could be qualified by the requirement that small businesses need only take reasonable steps to comply with the privacy principles. This would allow the Privacy Commissioner to issue guidance on what steps (if any) a small business should take to be deemed to have made a reasonable effort to comply.[82]

39.44 Other stakeholders suggested that the impact of the *Privacy Act* on small businesses could be reduced by:

- a privacy code for small businesses, which would relax or remove bureaucratic aspects of the *Privacy Act* while ensuring that personal information is handled appropriately;[83]

- public interest determinations issued by the Privacy Commissioner;[84] or

- specific exceptions to the privacy principles in relation to small businesses.[85]

EU adequacy

39.45 The small business exemption is one of the major obstacles to Australia's privacy laws being recognised as 'adequate' by the EU. This arguably impedes trade with the EU.[86]

39.46 Several stakeholders argued that removing the small business exemption would help to ensure that Australia's privacy laws were recognised as adequate by the EU.[87]

---

81 Government of South Australia, *Submission PR 565*, 29 January 2008.

82 Privacy NSW, *Submission PR 468*, 14 December 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

83 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007.

84 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

85 Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

86 One of the express objectives of the private sector provisions of the *Privacy Act* was to facilitate trade with the EU: Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 16.

87 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Bankers' Association Inc, *Submission PR 259*,

Some stakeholders submitted that Australian privacy laws should be consistent with international standards.[88] For example, the Public Interest Advocacy Centre (PIAC) submitted that removal of the exemption would bring Australia in line with other comparable jurisdictions, including the United Kingdom, Canada and New Zealand.[89]

39.47 Professor Graham Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that a European company would not be able to ascertain readily whether a business is an exempt small business for the purposes of the *Privacy Act*. They stated that:

> If personal data are transferred from Europe to some proper recipient in Australia, there is nothing in the *Privacy Act* except the normal rules governing secondary purposes to prevent the data from being disclosed to an exempt small business operator.[90]

39.48 The Australian Bankers' Association (ABA) noted that the lack of EU adequacy has significant disadvantages for Australian companies that operate in a European environment. This is because an Australian company would have to comply with the EU Directive by fulfilling certain conditions on a case-by-case basis when transferring data from an EU country to Australia. The ABA submitted that removing the small business exemption would eliminate a significant impediment to a finding of EU adequacy.[91]

39.49 The National Australia Bank and MLC Ltd submitted that, as Australia's privacy laws are not recognised as adequate by the EU, Australian businesses that wish to trade with organisations in the EU have to bear the costs of additional contractual arrangements;[92] including the costs of periodic audits of compliance with these arrangements.[93]

---

19 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

88 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

89 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

90 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

91 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

92 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

93 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

39.50 In contrast, Australian Business Industrial stated that it was not aware of any instances where the small business exemption has had an adverse impact on those conducting business with EU organisations.[94] The Real Estate Institute of Australia (REIA) argued that Australia should not pursue a declaration of adequacy under the EU Directive if this comes at the cost of removing the small business exemption.[95]

Removing the exemption for high-risk sectors

39.51 There are significant concerns that certain small businesses pose a particularly high risk to privacy.[96] Examples of such businesses included those in the telecommunications industry (such as ISPs); debt collectors; and small businesses that are handling personal information by reason of the application of the *Northern Territory Emergency Response Act* and related legislation.[97]

Telecommunications industry

39.52 The OPC Review recommended that the Attorney-General consider regulations to ensure that the *Privacy Act* applies to all small businesses in the telecommunications sector.[98] In response, the Australian Government stated that the Attorney-General's Department would, in conjunction with the relevant government agencies, consider making regulations to ensure that the *Privacy Act* applies to such businesses.[99]

39.53 The Senate Committee privacy inquiry expressed concern that regulating small businesses in some areas—such as residential tenancy databases and telecommunications—but not others would add to the complexity of the legislation.[100]

39.54 In submissions to this Inquiry, the Department of Broadband, Communications and the Digital Economy (DBCDE), ACMA and other stakeholders expressed particular concern that small business operators in the telecommunications industry are exempt from the operation of the *Privacy Act*.[101]

---

94 Australian Business Industrial, *Submission PR 444*, 10 December 2007.

95 Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007.

96 See, eg, Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; 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; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

97 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

98 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 9, 15, 52.

99 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 3.

100 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32].

101 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; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

39.55 The DBCDE submitted that, from a policy perspective, all businesses in the telecommunications industry should be subject to privacy regulation, regardless of size. It noted that a high proportion of providers in the telecommunications industry are small business operators—and therefore exempt from the operation of the *Privacy Act*. The DBCDE noted that the *Telecommunications Act 1997* (Cth) regulates the use and disclosure of information, but not other aspects of information handling. In addition, some small businesses operating in association with the telecommunications industry may not be subject to Part 13 of the *Telecommunications Act*, the *Privacy Act* or any relevant industry code. Consequently, the DBCDE expressed support for the ALRC's proposal to remove the small business exemption.[102]

39.56 Other stakeholders supported the removal of the small business exemption as a way to address privacy concerns raised in relation to ISPs.[103] For example, ACMA noted that more than a quarter of ISPs are small business operators. It questioned the relevance of this exemption in the increasingly convergent telecommunications environment.

> Most consumers have little or no knowledge of the exemptions to the *Privacy Act*. As a consequence, many consumers transact with businesses assuming that their personal information is protected by the *Privacy Act*, when this may not be the case. If the small business exemption is to continue, it may be beneficial to publicise the exemption. This activity may result in voluntary compliance becoming a key market differentiator.[104]

39.57 The Communications Alliance conceded that there were operators in the telecommunications sector that fell within the small business exemption and were not subject to privacy regulation. It submitted, however, that the problem should be resolved by raising awareness about privacy issues and providing education and incentives to the industry for voluntary adoption of the NPPs, rather than additional privacy regulation that increases the regulatory burden on small operators.[105]

Debt collectors

39.58 The *Privacy Act* generally does not apply to debt collectors that have an annual turnover of $3 million or less. A debt collection organisation that has purchased debts from a credit provider, however, may be subject to the credit reporting provisions of the Act. In addition, debt collection organisations are regulated by the consumer protection provisions of the *Trade Practices Act 1974* (Cth), the *Australian Securities and Investments Commission Act 2001* (Cth) and other relevant state legislation.[106]

---

102 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007. See also Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

103 Australian Digital Alliance, *Submission PR 422*, 7 December 2007; Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

104 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

105 Communications Alliance Ltd, *Submission PR 198*, 16 February 2007.

106 The Australian Competition and Consumer Commission and the Australian Securities and Investments Commission, who are jointly responsible for enforcing consumer protection legislation in relation to the

39.59 The Consumer Credit Legal Centre (NSW) (CCLC) submitted that a small business exemption should not apply in relation to debt collection, because when a bank sells the debt to a debt collector who is covered by the small business exemption, 'the strict confidentiality the consumer expected when entering into the loan has now been eroded often without their knowledge'. The CCLC contended that 'a consumer should be able to expect that the privacy rights that consumer had upon entering the loan are preserved for the life of the debt'.[107]

39.60 On the other hand, Abacus-Australian Mutuals (Abacus)—while acknowledging that debt collection activity may fall under the small business exemption even though the debtor borrowed from a larger financial institution—suggested that:

> The 2005 renewal of the ASIC/ACCC Debt Collection Guidelines does, in [our] view, provide some confidence that creditors will ensure any debt recovery action is undertaken in accord with privacy measures.[108]

Northern Territory National Emergency Response

39.61 In August 2007, the *Northern Territory National Emergency Response Act* and related legislation were passed to address issues of drug abuse and child sexual assault in the Northern Territory. The suite of legislation introduced a number of measures that involve the collection, use and disclosure of personal information by certain agencies and organisations, including exempt small businesses. Privacy and other human rights advocates have identified a number of privacy issues concerning these measures—in particular, measures contained in the *Northern Territory National Emergency Response Act* and the *Social Security and Other Legislation Amendment (Welfare Payment Reform) Act 2007* (Cth).[109]

39.62 Under s 20(5) of the *Northern Territory National Emergency Response Act*, licensees and their employees are required to collect certain personal information before selling liquor for consumption away from the licensed premises. The personal information to be collected includes the purchaser's name and address, and the name and address of the place where the purchaser proposes to consume the alcohol. Section 21 of the Act also requires a licensee to keep records of the personal

---

debt collection industry, have issued guidance to assist collectors and creditors in understanding how the legislation applies to them: Australian Competition and Consumer Commission and Australian Securities and Investments Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005). Issues concerning the application of the credit reporting provisions of the Act to debt collectors are discussed in Ch 57.

107 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

108 Abacus–Australian Mutuals, *Submission PR 174*, 6 February 2007, referring to Australian Competition and Consumer Commission and Australian Securities and Investments Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005).

109 Office of the Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs, Inquiry into the Northern Territory National Emergency Response Bill 2007 and Related Bills*, 1 August 2007; Aboriginal and Torres Strait Islander Social Justice Commissioner, *Social Justice Report 2007* (2008), Ch 3. See also Office of the Victorian Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Northern Territory National Emergency Response Bill 2007 and Related Bills*, 10 August 2007.

information collected for at least three years after the records are made, and to produce the records to an inspector upon demand.

39.63 In addition, s 27 of the Act requires a 'responsible person' for a publicly funded computer to ensure that a record is kept of each person who uses the computer, and the time and day of use.[110] A 'publicly funded computer' means a computer that is: owned or leased by an individual or body that received funding from a federal, state, territory or local government authority; on loan from a body that receives such funding; or owned or leased by an individual or a body that receives money directly or indirectly from the Australian Government under an arrangement to deliver employment-related services or programs.[111]

39.64 Where the 'responsible person' is a small business not acting under a Commonwealth contract it may fall within the small business exemption, for example, small businesses that receive funding from a state, territory or local government authority, and those that borrow a publicly funded computer from a government-funded body.

39.65 The OPC's submission to the inquiry by the Senate Standing Committee on Legal and Constitutional Affairs into the Northern Territory National Emergency Response Bill 2007 (Cth) and related bills (NT National Emergency Response inquiry)[112] noted that, although it was not clear what proportion of these licensees and responsible persons would be small businesses, it is possible that some of them could come within the definition of 'small business operator' and therefore fall outside the coverage of the *Privacy Act*. The OPC stated that, as a result, 'it would appear there may be a gap in statutory privacy protections applying to information collected and handled under these provisions'.[113]

39.66 The *Social Security and Other Legislation Amendment (Welfare Payment Reform) Act 2007* (Cth) amended social security law to set up an income management regime for recipients of certain welfare payments. Under this regime, whole or parts of certain welfare payments are set aside and directed to meet the priority needs of certain welfare recipients, as well as those of the recipient's partner, children and other dependants.[114] The legislation provides for certain powers in the collection, use and

---

110 *Northern Territory National Emergency Response Act 2007* (Cth) s 27. A 'responsible person' in this context means the individual, or the head of the entity, that has custody and control of the computer: *Northern Territory National Emergency Response Act 2007* (Cth) s 3.

111 *Northern Territory National Emergency Response Act 2007* (Cth) s 3.

112 See Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Social Security and Other Legislation Amendment (Welfare Payment Reform) Bill 2007 and Four Related Bills concerning the Northern Territory National Emergency Response* (2007).

113 Office of the Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs, Inquiry into the Northern Territory National Emergency Response Bill 2007 and Related Bills*, 1 August 2007.

114 *Social Security (Administration) Act 1999* (Cth) s 123TB; *Social Security and Other Legislation Amendment (Welfare Payment Reform) Act 2007* (Cth) sch 1 item 17.

disclosure of personal information. For example, a person may disclose protected information[115] to another person who is responsible for the operation of a school if the protected information relates to the enrolment of children and their attendance at school.[116] Accordingly, a small business operating a private school may collect personal information about children without being subject to the requirements of the *Privacy Act*.

39.67 Further, small businesses operating community stores may be required to participate in the income management regime and handle personal information of welfare recipients to ensure that welfare payments are used to meet priority needs. To obtain a community store licence, community stores may be assessed on a number of matters, including their capacity to participate in, and their record of compliance with, the requirements of the income management regime.[117] In addition, they may be subject to licence conditions relating to the regime.[118] Although many community stores may be government-funded and therefore may have to comply with the *Privacy Act* as government contractors, those that are not government-funded may qualify for the small business exemption.

39.68 In its submission to NT National Emergency Response inquiry, the OPC stated that, where small businesses operating community stores are required to participate in the income management regime:

> The Office assumes this may require them to collect and possibly use or disclose personal information that could include financial or sensitive information. It may be that some of these businesses will not be subject to privacy regulation. The Office suggests that appropriate information handling practices based on privacy principles in the Privacy Act could be made part of the renewed licence conditions for these businesses.[119]

39.69 Having considered different aspects of the Northern Territory National Emergency Response Bill and related bills, the OPC submitted that:

> Given the sensitivities of much of the information that will be collected, used and disclosed under some of the provisions of the Bills the Office believes it is important

---

115 'Protected information' means information: (a) about a person that is or was held in the records of the Department of Families, Housing, Community Services and Indigenous Affairs or of the Commonwealth Services Delivery Agency; (b) about a person obtained by an officer under the family assistance law that is or was held in the records of the Australian Taxation Office (ATO), Medicare Australia or the Health Insurance Commission; or (c) to the effect that there is no information about a person held in the records of the Department of Families, Housing, Community Services and Indigenous Affairs, the Commonwealth Services Delivery Agency, the ATO or Medicare Australia: *Social Security Act 1991* (Cth) s 23.

116 *Social Security (Administration) Act 1999* (Cth) s 202(6); *Social Security and Other Legislation Amendment (Welfare Payment Reform) Act 2007* (Cth) sch 1 item 21.

117 *Northern Territory National Emergency Response Act 2007* (Cth) s 93.

118 Ibid s 103(1)(c).

119 Office of the Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs, Inquiry into the Northern Territory National Emergency Response Bill 2007 and Related Bills*, 1 August 2007.

> that consideration be given to ensuring that appropriate privacy safeguards are put in place for those entities not currently covered by statutory privacy regulation.[120]

39.70 In the *Social Justice Report 2007*, Mr Tom Calma, the Aboriginal and Torres Strait Islander Social Justice Commissioner, expressed concern about the inadequate privacy protection in the *Northern Territory National Emergency Response Act* and related legislation, including the fact that most small businesses are not regulated under the *Privacy Act*.[121] The Commissioner recommended that the income management scheme under the *Social Security and Other Legislation (Amendment (Welfare Payment Reform) Act* should be reviewed and amended to ensure compliance with human rights standards, including privacy protection.[122]

39.71 In its submission to this Inquiry, the Human Rights and Equal Opportunity Commission (HREOC) noted the OPC's concern that the passing of the *Northern Territory Emergency Response Act* and associated legislation resulted in a gap in privacy protection. HREOC submitted that Indigenous people may have no legal redress when there is an unauthorised use or disclosure of their personal information collected by a small business operator under the relevant legislation. HREOC submitted that removing the small business exemption would be one way of addressing this gap.[123]

Other industries or services

39.72 Some stakeholders suggested other high-risk sectors to which the small business exemption should not apply.[124] One particular area of concern is small businesses that work with children or young people.[125] The NSW Commission for Children and Young People expressed concern that services such as child care centres, family counselling or dispute resolution services—which often keep records of sensitive personal information of children and young people—may fall within the small business exemption. The Commission submitted that the *Privacy Act* should be amended to include specifically any business that provides services to children and young people.[126]

---

120 Ibid, 1.

121 Aboriginal and Torres Strait Islander Social Justice Commissioner, *Social Justice Report 2007* (2008), 278.

122 Ibid, rec 11(c), 298.

123 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.

124 G Poscoliero, *Submission PR 575*, 3 March 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007; NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007; AXA, *Submission PR 119*, 15 January 2007; Confidential, *Submission PR 97*, 15 January 2007.

125 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007; NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007.

126 NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007.

39.73 Youthlaw noted that community service organisations that are small business operators are not covered by either federal or state privacy legislation unless they are contracted service providers to a government agency.

> As a result young people, children and families may be wary about seeking help and providing information to these agencies if they believe this information is not subject to privacy legislation.[127]

39.74 The OPC suggested that consideration should be given to extending, or clarifying, the application of the *Privacy Act* to child care centres and family counselling and dispute resolution services.[128]

39.75 Other stakeholders raised concern about the application of the small business exemption to other types of small businesses, including:

- real estate agents;[129]
- dating agencies;[130]
- recruitment agents;[131]
- small businesses that provide computer data maintenance services;[132]
- small businesses that collect and use biometric information;[133] and
- small businesses that have control over large amounts of personal information and access to the credit reporting system,[134] such as financial services providers.[135]

---

127 Youthlaw, *Submission PR 390*, 6 December 2007.

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

129 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

130 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

131 Confidential, *Submission PR 97*, 15 January 2007. Although recruitment organisations trade in personal information, under s 6D(7)(a) of the *Privacy Act*, a recruitment organisation that has an annual turnover of $3 million or less may still be covered by the small business exemption if it has the consent of the individuals concerned. It also should be noted that the acts and practices of a recruitment organisation do not fall within the employee records exemption, unless they are in relation to the employee records of a current or former employee of that recruitment organisation and are directly related to that current or former employment relationship: see Information Technology Contract & Recruitment Association, *Privacy and the Recruitment Industry* <www.itcra.com/index.asp?menuid=100.010&artid=119> at 19 May 2008. The employee records exemption is discussed in Ch 40.

132 G Poscoliero, *Submission PR 575*, 3 March 2008.

133 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

134 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007; AXA, *Submission PR 119*, 15 January 2007.

135 AXA, *Submission PR 119*, 15 January 2007. The ALRC notes that the small business exemption generally does not apply to private investigators, as they trade in personal information without the consent of the individuals concerned: see *Privacy Act 1988* (Cth) s 6D(4)(c), (d), (7), (8). Privacy issues relating to private investigators are discussed in detail in Ch 44.

Arguments for retaining the exemption

39.76 A number of stakeholders opposed the ALRC's proposal to remove the small business exemption.[136] The main arguments for retaining the small business exemption are based on a view that it is necessary to achieve an appropriate balance between privacy protection and the ability of the small business sector to operate efficiently.[137] In particular, it was suggested that many small businesses pose a low risk to privacy because they do not: collect a significant amount of personal information; deal inappropriately with personal information; or handle much personal information that pose a high risk to privacy.[138]

39.77 Finally, there were concerns that removing the exemption would increase significantly the overall regulatory burden and compliance costs on small businesses.[139] Stakeholders had differing views on the extent and implications for small businesses of the costs of complying with the *Privacy Act*. Compliance costs are discussed later in this chapter.

Balancing privacy risks and compliance burden

39.78 The OPC stated that the small business exemption is 'necessary to balance privacy protection against the need to avoid unnecessary cost on small business'.[140]

---

136 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; CPA Australia, *Submission PR 476*, 14 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007 (endorsed by Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007); Australian Business Industrial, *Submission PR 444*, 10 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

137 CPA Australia, *Submission PR 476*, 14 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

138 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; CPA Australia, *Submission PR 476*, 14 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

139 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; Australian Institute of Company Directors, *Submission PR 424*, 7 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007.

140 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007, referring to Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), ii.

The OPC submitted that requiring many small businesses to comply with the NPPs would be impractical and create an unnecessary compliance burden.[141]

39.79 The OPC cited research undertaken by the Regulation Taskforce, which showed that compliance matters generally can consume up to 25% of the time of large companies and that the impact would be even greater for small businesses that do not have the in-house capacity to keep abreast of large amounts of regulation.[142] It argued that the small business exemption should not be removed unless the benefit to individuals from the imposition of this compliance burden on small businesses can be demonstrated.[143]

Privacy risks

39.80 Some stakeholders highlighted the low risk to privacy posed by most small businesses. The Motor Trades Association of Australia submitted that small businesses generally only handle and retain personal information for purposes that are related to the transaction initiated on behalf of the consumer, 'to comply with existing legal requirements or to further the relationship between the consumer and the small business operator'.[144]

39.81 The Council of Small Business of Australia (COSBOA) argued that, compared to larger businesses, small businesses have fewer customers, fewer outlets, fewer complementary business interests, smaller market share and fewer staff—all of which means that they handle a lower volume of personal information, have less reason or need to disseminate information, and that additional time spent on regulatory activities carries a high opportunity cost.[145] The REIA argued that, while exemptions are blunt instruments, regulating an entire sector of business, the majority of which pose low risks to privacy, was an even blunter approach.[146]

39.82 Some stakeholders submitted that there was no evidence that small business operators have handled personal information inappropriately.[147] For instance, the REIA argued that the level of privacy complaints relating to small businesses were proportionately lower than for larger businesses, given the sheer number of small businesses and their share of total sales and services.[148]

---

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

142 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007, referring to Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), ii.

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

144 Motor Trades Association of Australia, *Submission PR 470,* 14 December 2007.

145 Council of Small Business of Australia, *Submission PR 389,* 6 December 2007.

146 Real Estate Institute of Australia, *Submission PR 400,* 7 December 2007.

147 Motor Trades Association of Australia, *Submission PR 470,* 14 December 2007; Australian Business Industrial, *Submission PR 444,* 10 December 2007; Australian Institute of Company Directors, *Submission PR 424,* 7 December 2007.

148 Real Estate Institute of Australia, *Submission PR 400,* 7 December 2007.

39.83 Similarly, Australian Business Industrial submitted that there was no evidence to suggest that small businesses are abusing the exemption, or that personal information held by small businesses was 'exploited or mishandled in any significant, systematic or serious manner'. It argued, therefore, that the removal of the exemption was not a justified or proportional response to any perceived privacy risks.[149]

39.84 The Department of Employment and Workplace Relations (DEWR) (now the Department of Education, Employment and Workplace Relations) suggested that, even if small businesses were to misuse personal information, the consequences of such misuse generally would be less severe than those resulting from misuse of personal information by large organisations or the government.[150]

39.85 Other stakeholders expressed the view that additional privacy requirements on small businesses are unnecessary because small businesses already take steps to ensure that the personal information of customers is handled appropriately.[151] The Victorian Automobile Chamber of Commerce (VACC) suggested that 'reputation and repeat business are essential for small businesses to survive. It is therefore in their best interests to handle information appropriately'.[152]

39.86 The Financial Planning Association of Australia submitted that imposing privacy requirements on small businesses would not increase significantly consumer protection or confidence in small businesses. It argued that such additional requirements could inhibit commercial activities in certain circumstances—for example, where customers have no privacy concerns about the relevant transactions and the risk to privacy is minimal.[153]

39.87 Some stakeholders submitted that the small business exemption should be retained because there are mechanisms in the *Privacy Act* that limit the application of the exemption in appropriate circumstances, by excluding those small businesses that:

- engage in activities that pose a high risk to privacy, such as private sector health service providers and small businesses that trade in personal information;[154]

149 Australian Business Industrial, *Submission PR 444*, 10 December 2007.

150 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.

151 Australian Retailers Association, *Submission PR 131*, 18 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

152 Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

153 Financial Planning Association of Australia, *Submission PR 496*, 19 December 2007.

154 CPA Australia, *Submission PR 476*, 14 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

- enter into certain business relationships, for example, with government or larger organisations;[155]

- have been brought under the jurisdiction of the *Privacy Act* through an amendment of the Act, for instance, small businesses that are 'reporting entities' within the meaning of the AML/CTF Act;[156]

- have been prescribed as an 'organisation' by regulations made under s 6E of the *Privacy Act*, such as residential tenancy database operators;[157] and

- voluntarily opt in to coverage by the *Privacy Act* where there is a commercial or social benefit for the small business to do so.[158]

Compliance burden

39.88 Some stakeholders submitted that the proposed removal of the small business exemption is contrary to the stated policy intention of the Australian Government to reduce regulatory and compliance burdens on small businesses,[159] and would result in a more complex regulatory environment.[160]

39.89 On the other hand, while the OPC did not support removing the small business exemption, it conceded that the exemption 'may not promote consistency and may lead to additional burdens for small businesses and individuals because of the uncertainty it creates about whether personal information is regulated by the *Privacy Act*'.[161] The OPC also noted that, given personal information held by small businesses is covered by the Act where it has been collected for the purposes of the AML/CTF Act,[162]

> relevant small business will need to be able to distinguish between personal information that is regulated, and that which is not. The Office considers that many small business reporting entities may find that compliance is simplified by treating all personal information as though it is covered by the *Privacy Act*.[163]

---

155 CPA Australia, *Submission PR 476*, 14 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

156 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

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

158 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

159 See, eg, Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

160 Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

161 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007, referring to Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), ii.

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

163 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

39.90 Several stakeholders suggested that removing the exemption also could have a number of adverse consequences, including: reduced ability of small businesses to compete with larger competitors;[164] price increases or decreased level of services for consumers;[165] reduced profitability, which could impact on employment levels;[166] and increased small business failure and economic inefficiency.[167]

39.91 Some stakeholders also raised concerns about the timing of the removal of the small business exemption.[168] The Australian Industry Group (AIG) and the Australian Electrical and Electronic Manufacturers' Association (AEEMA) expressed concern that removing the small business exemption would extend the coverage of the *Privacy Act* in a very short time and result in a significant increase in the compliance burdens on both the small business sector and the OPC.[169] COSBOA submitted that removing exemption provisions under the *Privacy Act* should be considered in the context of the new simplified Act proposed by the ALRC, rather than concurrently.[170]

Issues involved in retaining the exemption

39.92 If the small business exemption is to be retained, a number of issues may require further consideration. These include: whether the existing definition of a 'small business' is appropriate; whether the consent provisions under s 6D(7) and (8) of the *Privacy Act* should be removed; and whether the voluntary opt-in mechanism should be preserved.

---

164 Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

165 Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

166 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007. See also Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

167 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

168 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

169 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007.

170 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

Definition of a 'small business'

39.93 Many stakeholders identified the definition of 'small business' as problematic. In submissions and consultations, there was recognition—by both proponents and opponents of the small business exemption—that the threshold for the small business exemption of an annual turnover of $3 million or less is arbitrary.[171]

39.94 A number of stakeholders suggested that the current threshold of $3 million annual turnover is too low.[172] The VACC submitted that, in 2004:

> small businesses within the automotive industry estimated an annual turnover of approximately $6–7 million despite recording minimum profit margins. Given the high cost of vehicles which are generally greater than $20,000, it is not difficult for small businesses to exceed the $3 million threshold.[173]

39.95 The REIA and COSBOA suggested that the threshold for the exemption should be raised to $5 million. This reflects the ongoing impact of inflation,[174] the recent period of economic prosperity that was likely to have lifted the annual turnover of many small businesses,[175] and the fact that there has been no change to the threshold for the exemption since the introduction of the *Privacy Act*.[176] The REIA submitted that raising the threshold for the exemption to $5 million would ensure that the threshold could be left unchanged over the short term.[177]

39.96 In contrast, other stakeholders expressed the view that the threshold for the small business exemption should be lowered.[178] The Arts Law Centre of Australia suggested that the threshold for the exemption should be reduced to an annual turnover of $500,000 or less in order better to achieve a balance between protecting the privacy interests of individuals and the needs of small businesses.[179]

---

171 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Council of Small Business Organisations of Australia Ltd, *Submission PR 203*, 21 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

172 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

173 Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

174 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

175 Ibid.

176 Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

177 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

178 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007 (endorsed by Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007); S Hawkins, *Submission PR 382*, 6 December 2007.

179 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007 (endorsed by Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007). See also S Hawkins, *Submission PR 382*, 6 December 2007.

39.97 One stakeholder noted that defining small business based on turnover was at odds with the definition adopted by both the ABS and the Australian Taxation Office. It was suggested that, if an exemption were to be retained, the definition should be based on the level of risk that an organisation poses to privacy. The exemption could apply on the basis of particular types of information held by the organisation or the number of individuals about whom personal information is held.[180]

39.98 The OPC reiterated its recommendation in the OPC Review that the definition of small business be expressed in terms of the ABS definition of small business.[181] There was some opposition to the OPC's recommendation.[182] The Australian Chamber of Commerce and Industry (ACCI) argued that the test recommended by the OPC would capture many small businesses that are currently exempt from the operation of the *Privacy Act*, because casual or part-time employees would be counted as a single employee. The ACCI submitted that this would have a particularly serious impact on many service industries, as they rely heavily on casual labour.[183]

39.99 The Australian Privacy Foundation stated that it was impossible to envisage any sensible size or other criteria which would capture all information-handling activities that pose a high risk to privacy while excluding those activities that pose a low risk to privacy. It was argued that even businesses operated by a single individual, such as private investigators and operators of specialised websites, could be engaging in privacy-intrusive activities.[184]

39.100 Electronic Frontiers Australia opposed an exemption based on the number of employees because 'this would still result in exemption for organisations that collect and disclose substantial amounts and types of personal information'.[185] In common with the Australian Privacy Foundation, Electronic Frontiers Australia argued that even a sole trader may handle large amounts of personal information.[186]

39.101 The Treasury noted that a single definition of a 'small business entity' was introduced on 1 July 2007 to align the definition across various pieces of tax legislation.[187] It suggested that the adoption of this definition in the *Privacy Act* would

---

180 Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007.

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

182 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

183 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.

184 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

185 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

186 Ibid.

187 Before the introduction of the *Tax Laws Amendment (Small Business) Act 2007* (Cth), there were separate criteria for small business entities to determine their eligibility for a number of different tax concessions, including concessions related to the goods and services tax, the capital gains tax and the fringe benefits tax. In 2007, the *Tax Laws Amendment (Small Business) Act* was passed to standardise the eligibility criteria for small business to access concessions for all taxation purposes: see *Tax Laws Amendment (Small Business) Act 2007* (Cth) s 328-10. This was achieved by the creation of a single definition of a

promote the alignment of all definitions of 'small business' in federal legislation and ensure that more businesses would fall within the purview of the *Privacy Act*. The Treasury also advised that, during the implementation of the *Tax Laws Amendment (Small Business) Act 2007* (Cth), the ABS indicated its intention to adopt the definition of 'small business' under tax legislation, despite the fact that it would continue to collect data on businesses by classifying them on the basis of the number of people they employ.[188]

Consent provision

39.102 If the small business exemption were to be retained, another issue for consideration is whether the consent provisions under s 6D(7) and (8) of the *Privacy Act* should be removed. These subsections provide that a small business that trades in personal information may still be exempt if it has the consent of the individuals concerned to collect or disclose their personal information.[189]

39.103 The OPC Review recommended the removal of the consent provisions on the basis that the provisions were 'clumsy and complicated', and that there was a lack of certainty as to whether a single failure to gain consent would change the exempt status of the business.[190] In the OPC's view, this also would ensure that all organisations that trade in personal information would be regulated by the *Privacy Act*, and that public number directory producers could not make use of the exemption.[191]

39.104 The Australian Government disagreed with the OPC Review's recommendation, however, on the basis that 'the Act currently provides a mechanism for dealing with situations in which the consent provisions should not operate'.[192]

'small business entity' based on an aggregated annual turnover of less than $2 million: *Tax Laws Amendment (Small Business) Act 2007* (Cth) sch 1.

188 Australian Government Treasury, *Submission PR 581*, 20 March 2008.

189 *Privacy Act 1988* (Cth) s 6D(7), (8).

190 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 185, rec 53.

191 Ibid, 62, 185. Public number directory producers are authorised to access data concerning listed telephone numbers from the Integrated Public Number Database, a database of all listed and unlisted public telephone numbers in Australia: Australian Government Department of Broadband, Communications and the Digital Economy, *Integrated Public Number Database (IPND)* <www.dbcde.gov.au/communications_and_technology/policy_and_legislation/numbering> at 23 April 2008. Public number directory producers are persons who: (i) compile, publish, maintain or produce directories of public numbers; (ii) provide directory assistance services; or (iii) supply goods or services which are a combination of (i) and (ii): Australian Communications Authority, *Telecommunications (Section of the Telecommunications Industry) Determination*, 25 September 1998.

192 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 10.

Voluntary compliance and opting in

39.105 Retaining the small business exemption also raises the issue of whether the voluntary opt-in mechanism—which allows a small business operator to opt in to coverage by the *Privacy Act*[193]—should be preserved. In practice, some small businesses appear to have committed to comply voluntarily with the *Privacy Act* without using the opt-in mechanism, for example, by posting Privacy Policies on their websites, or by agreeing to contractual terms that require them to comply with the *Privacy Act*. In a number of case studies, it was observed that some small businesses have Privacy Policies that state that they are bound by the *Privacy Act* even though they have not opted in.[194] It has been argued that, since such small businesses have not opted in formally, this leaves consumers or the other contracting party with limited avenues of complaint.[195]

39.106 Some stakeholders supported retaining the opt-in procedure.[196] The OPC suggested that there are a number of benefits in retaining the opt-in provisions, in that the provisions allow small businesses to:

- show their commitment to privacy, which could enhance their brand and community trust in their operations;
- apply for a privacy code under s 18BA of the *Privacy Act*;
- fulfil a condition of signing up to a code that is not connected to the Act, such as the *Credit Union Code of Conduct*; and
- apply to the Privacy Commissioner for a Public Interest Determination (PID), as s 73 of the *Privacy Act* requires that an applicant for a PID must be an organisation.[197]

39.107 The OPC suggested that, instead of removing the exemption, small businesses that do not handle large amounts of personal information should be encouraged to opt in to coverage by the *Privacy Act*. Further, the OPC could assist small businesses by

---

193 *Privacy Act 1988* (Cth) s 6EA.

194 M Jackson and others, *Small Business: Issues of Identity Management, Privacy and Security* (2006), 9–10.

195 Ibid, 9–10.

196 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Australian Retailers Association, *Submission PR 131*, 18 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007. The OPC submitted that the opt-in mechanism also should be extended so that other entities, such as registered political parties, have the ability to opt-in to coverage of the NPPs: Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

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

promoting the benefits of embedding relevant privacy practices into their business operations and encouraging good privacy practice.[198]

39.108 DEWR submitted that the opt-in mechanism represents

> a market solution to the question of which small businesses should monitor and control their handling of personal information …
>
> there is a role for privacy-savvy customers and other organisations having business dealings with small business to alert small business to privacy concerns, and to use their market power to persuade small business to 'opt in' or otherwise incorporate privacy safeguards in their business practices.[199]

39.109 The ACCI stated that it would not oppose an opt-in mechanism, provided that it remains voluntary. It suggested, however, that given the low take-up of the opt-in procedure by small businesses, the procedure should be discontinued if the cost is disproportionate to the benefit of opting in.[200]

39.110 The ABA submitted that the opt-in mechanism would not be required if the Privacy Commissioner were to develop a PID modifying the application of the NPPs to small businesses.[201]

Compliance costs

39.111 'Compliance costs' are defined as 'the direct costs to businesses of performing the various tasks associated with complying with government regulation'.[202] One of the main arguments in favour of retaining the small business exemption is that previously exempt small businesses would incur significant compliance costs to ensure that they meet their obligations under the *Privacy Act*.

39.112 Business has identified privacy requirements as an important contributor to their cumulative regulatory burden. In its 2006 report, *Rethinking Regulation*, the Productivity Commission's Taskforce on Reducing Regulatory Burdens on Business recommended that the Australian Government consider the impact of privacy requirements on business compliance costs in the context of a wider review of Australian privacy laws.[203]

39.113 In its 2006 report, *The Victorian Regulatory System*, the Victorian Competition and Efficiency Commission (VCEC) noted the challenge for government

---

198 Ibid.

199 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

200 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

201 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

202 Australian Government, *Best Practice Regulation Handbook* (2007), 26.

203 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.

in assisting small businesses in complying with regulation, given the need to provide adequate protection to consumers, workers and the environment:

> There are a number of ways of meeting this challenge. In some cases, there may be less onerous provisions in the regulations which relate to small businesses … or even exemptions … However, such approaches by favouring some businesses over others can distort markets, and discourage smaller businesses growing past such thresholds. Another approach, advocated by the United Kingdom's Better Regulation Taskforce was to 'think small first' based on the assumption that regulation designed with the capacity and constraints of small business in mind would also be readily implemented by larger businesses.[204]

39.114 The VCEC went on to note that 'another approach is to have a consistent regulatory system but to provide special assistance for smaller businesses'.[205]

Submissions and consultations

39.115 Many business and industry groups expressed concern that removing the small business exemption would increase the overall regulatory burden and compliance costs on small businesses.[206] For example, Australian Business Industrial submitted that, in a 2007 survey by the NSW Business Chambers,

> 77% of respondents reported that the cost of compliance with government regulations was of moderate or major concern in the context of their business, and 47% of respondents reported that specifically, compliance with privacy requirements was of moderate or major concern in the context of their business.[207] This is a high level of concern among our membership, particularly given that at this point in time, only approximately 45% of our members are currently required to comply with the NPPs.[208]

39.116 A number of stakeholders submitted that, if the small business exemption were removed, the costs of compliance would be significant.[209] It was suggested that the costs of compliance would include costs relating to:

---

204 Victorian Competition and Efficiency Commission, *The Victorian Regulatory System* (2006), 26–27.

205 Ibid, 27.

206 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

207 See NSW Business Chambers, *2007 Australian Business Priorities—Fixing the Federation* (2007), 20.

208 Australian Business Industrial, *Submission PR 444*, 10 December 2007.

209 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; AXA, *Submission PR 119*, 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

- initial familiarisation with the new privacy regime;[210]
- conducting an initial privacy audit and a legal review;[211]
- developing a Privacy Policy;[212]
- obtaining advice from external sources, such as legal advice;[213]
- training and educating staff,[214] and appointing staff members to the role of privacy officers;[215]
- purchasing and maintaining information technology systems and administrative items to facilitate record keeping, such as filing cabinets that can be locked, paper shredders and computer software;[216]
- handling customers' requests and complaints,[217] and obtaining consent from individuals for the collection and use of their personal information;[218]
- maintaining the security of personal information held and keeping such information up-to-date;[219] and
- conducting periodic privacy audits to delete records that are no longer required.[220]

39.117 In addition, the REIA submitted that removing the exemption would result in lost business opportunities in circumstances where restrictions on the use of information precludes normal activities that violate the Unified Privacy Principles (UPPs).[221]

---

210 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.
211 Ibid.
212 Ibid.
213 Retail Motor Industry, *Submission PR 407*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.
214 Retail Motor Industry, *Submission PR 407*, 7 December 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.
215 Retail Motor Industry, *Submission PR 407*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.
216 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.
217 Ibid; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.
218 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.
219 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.
220 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.
221 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

39.118 Some stakeholders noted that certain compliance costs would be ongoing, including the cost of: implementing and updating the Privacy Policy;[222] keeping abreast of changes to privacy regulation;[223] dealing with customers' complaints;[224] and management and staff time for reporting and training.[225]

39.119 The ACCI submitted that the total fixed costs to establish a simple privacy regime for an individual small business would be $3,500. It stated that:

> Estimates of the legal costs for drafting a rudimentary privacy policy in 2007, though again tempered by the fact that the cost could vary considerably depending upon the characteristics of the business, were approximated at $2500. Supporting documentation, in terms of reference material such as the *Federal Privacy Handbook* and the *Privacy [Compliance] Toolkit* would now cost an additional $1000.[226]

39.120 Several stakeholders submitted that small businesses would be affected disproportionately by the need to comply with the *Privacy Act* compared to larger businesses because they do not have the same capacity and resources to comply with their regulatory obligations.[227] For example, the ACCI suggested that small businesses: have a narrower revenue base over which to spread the fixed costs of compliance; may not have in-house regulatory expertise to assist with compliance; may lack the time to keep abreast of regulatory developments; and may be discouraged by the complexity of regulation and the threat of penalties for even inadvertent non-compliance. The ACCI was of the view that regulation also can cause businesses to adjust their processes in ways that add to costs, and can make some commercial pursuits less viable or attractive.[228]

39.121 The AIG and AEEMA submitted that the compliance burden would fall disproportionately heavily on small businesses, because most of the costs involved would be fixed costs, which apply regardless of the size of the business.[229]

39.122 Other stakeholders submitted that any reform of the exemption should be subject to an appropriate consultation process. Abacus submitted that there should be appropriate consultation with affected industries and industry bodies to consider

---

222 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.
223 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.
224 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.
225 Retail Motor Industry, *Submission PR 407*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.
226 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.
227 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; Australian Institute of Company Directors, *Submission PR 424*, 7 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007. See also Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; AXA, *Submission PR 119*, 15 January 2007.
228 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.
229 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007.

compliance and implementation issues and ensure that compliance costs would not be substantial.[230] Similarly, the Queensland Government submitted that the Australian Government should undertake significant consultation and develop strategies to assist small businesses before the removal of the exemption.[231]

39.123 The Government of South Australia suggested that any compliance costs would be proportional to the business size—if business operations were small, the costs of compliance would be low. It further noted that there are many ways to reduce unnecessary costs of compliance without having an exemption, such as providing small businesses with guidance on records management and collection.[232]

> As many small businesses do not have significant holdings of personal information, the effect of removing the exemption on the cost burden of compliance is not expected to be significant … Minimising compliance costs should focus on unnecessary compliance cost, not compliance cost per se. There may be different ways and means to minimize unnecessary compliance costs, such as effective business awareness raising [and] more detailed and practical guidance from relevant government agencies, particularly the Office of the Federal Privacy Commissioner (through provision of sample privacy policies, manuals and training kits).[233]

39.124 PIAC noted that some small businesses, such as certain government-funded community organisations, already are required to comply with the *Privacy Act*. PIAC stated that, although such organisations received neither additional funding nor tax benefits to cover the costs of compliance, they did not have any difficulty in meeting their privacy obligations. PIAC submitted, therefore, that any argument that the exemption should not be removed on the basis of compliance costs is flawed.[234]

Estimated costs of compliance

39.125 In October 2007, the Office of Small Business (OSB) provided the ALRC with an estimate of the compliance costs for small businesses in the event that the small business exemption were to be removed.[235] The OSB estimated that the removal of the small business exemption would affect 1,805,000 businesses and result in a total cost on small business of $3.186 billion. The OSB also estimated that each small business would incur a start-up cost of $842 and an ongoing cost of $924 per year.[236]

---

230 Abacus–Australian Mutuals, *Submission PR 174*, 6 February 2007.
231 Queensland Government, *Submission PR 490*, 19 December 2007.
232 Government of South Australia, *Submission PR 187*, 12 February 2007.
233 Ibid.
234 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
235 The estimate was calculated using the Australian Government Business Cost Calculator: Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007). The Australian Government Business Cost Calculator is an information technology-based tool designed to assist policy officers in estimating the compliance costs of different policy options on businesses: Australian Government, *Best Practice Regulation Handbook* (2007), 26.
236 Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007).

39.126 In January 2008, the ALRC engaged an external consultant, Applied Economics, to provide an independent assessment of the likely costs of compliance that would result from the removal of the small business exemption.[237] The detailed cost estimate prepared by Applied Economics is attached to this Report as Appendix 4.

39.127 Applied Economics reviewed the OSB's cost estimates and concluded that it overestimated both the number of businesses that would be affected by the removal of the exemption and the average compliance costs that would be incurred by an affected business. Applied Economics estimated that the removal of the small business exemption would affect about 1,685,000 businesses and result in a total cost on small business of $0.88 billion. It also estimated that each affected business would incur a start-up cost of $225 and ongoing annual costs of $301.

Number of business affected

39.128 One of the main differences between the estimates prepared by the OSB and those prepared by Applied Economics concerned the number of small businesses that would be affected by the removal of the small business exemption. As noted by Applied Economics, this calculation is complicated because under the *Privacy Act* 'small business' is defined as a business with an annual turnover of $3 million or less, while the ABS only publishes data on the number of businesses with an annual turnover of less than $2 million. There are no hard data on the number of businesses with an annual turnover of between $2 million and $3 million.[238] It also is difficult to determine the number of businesses that do not hold any personal information about their staff or customers, and thus would be unaffected in any practical sense even if they were formally brought under the *Privacy Act*.

39.129 In addition, as noted above, a number of small businesses already are covered by the *Privacy Act*—such as small businesses that trade in personal information without the consent of the individuals concerned, and those that provide a health service and hold certain personal health information. Both the OSB and Applied Economics noted the difficulty in identifying the number of small businesses that currently are covered by the Act.[239]

39.130 In estimating the number of businesses that would be affected by the removal of the small business exemption, the OSB apparently used the number of businesses that employ up to 19 people as a proxy for the number of businesses with an annual turnover of $3 million or less. The OSB noted that, as at June 2006, there were approximately 1.88 million small businesses with less than 20 staff, and 75,000 small businesses that provided health services. By subtracting the number of small businesses

---

237 The Applied Economics cost estimate was prepared by Dr Peter Abelson and David Maynard. Notes on the authors appear in App 4.

238 Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), 20.

239 See Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007), 2; and the cost estimate prepared by Applied Economics in App 4 of this Report.

that provide health services from the estimated 1.88 million 'small businesses', the OSB estimated that 1,805,000 small businesses would be affected by the removal of the exemption.[240]

39.131 Applied Economics considered, however, that using the total number of businesses with up to 19 employees as a proxy for the number of businesses with an annual turnover of $3 million or less would be an overestimate. By analysing ABS data on the average turnover per employee, Applied Economics showed that in several industries, businesses with fewer than 20 employees could have a turnover of over $3 million. Since the ABS data shows that, as at June 2006, 1.84 million businesses had an annual turnover of less than $2 million, Applied Economics adopted the assumption that there are 1.86 million of businesses with an annual turnover of $3 million or less.[241]

39.132 Applied Economics also noted that, although the OSB subtracted 75,000 small health businesses to account for small businesses that do not qualify for the small business exemption, the OSB did not take into account other small businesses that would not be affected by the removal of the exemption—including those that already are ineligible for the exemption, and those that do not employ any staff and hold no personal information. For example, some non-employing businesses hold no personal information because they operate on the basis of cash transactions—such as butchers, greengrocers, corner shops, convenience stores and some tradespeople. Other non-employing businesses do not hold any personal information because they only provide goods and services to the business sector, instead of to individuals—for example, consultants, business tradespeople, and owners or operators of trucks. On this basis, Applied Economics estimated that a further 100,000 businesses would not be affected by the extension of the *Privacy Act* to the small business sector. Consequently, Applied Economics estimated that 1.685 million small businesses would be affected by the removal of the small business exemption.

---

240 Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007), 1, 3.

241 See App 4 of this Report.

Compliance tasks

39.133 The OSB estimated that small businesses would have to complete a total of 11 tasks in order to comply with the *Privacy Act*, including: familiarisation with privacy legislation; conduct of a privacy audit; development of a privacy plan; amendment of existing business documentation; training of staff; purchase of a filing cabinet; purchase of a paper shredder; handling of customer complaints; record keeping; promulgation of Privacy Policy; and update or review of a Privacy Policy.[242]

39.134 While Applied Economics accepted the 11 compliance tasks involved, and adopted the OSB's assumptions on the costs of labour,[243] it challenged some of the other assumptions. One of the major assumptions made by the OSB is that every small business would have to perform each of the 11 compliance tasks. For example, the OSB estimated that all 1.88 million small businesses would have to conduct two hours of privacy training for their staff, with 75% conducting the training 'in-house' at $26 per hour and 25% outsourcing this task to a professional at a cost of $100 each—resulting in a total weighted average cost of $89 for each small business.[244] As Applied Economics pointed out, however, the training of staff can apply only to businesses with employees. As at June 2006, there were 1,156,00 non-employing businesses in Australia. While this number includes some larger businesses that fall outside the small business exemption, the OSB's assumption that all of the small businesses would have to train staff seems unlikely. According to the estimate by Applied Economics, only 649,000 small businesses were employing businesses, and therefore the weighted average cost per business should be $34.[245]

39.135 Applied Economics also queried the estimated costs on two grounds: first, whether there may be other, less expensive, ways to perform each of the compliance tasks; and secondly, whether some businesses already have taken some of these steps before they were required to do so. By analysing the OSB's estimate on these two grounds, Applied Economics arrived at a lower average cost per business for 10 of the 11 compliance tasks. The following table compares the breakdown of the cost estimate prepared by the OSB and that prepared by Applied Economics:

---

242 Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007), 1.

243 The OSB estimated that the costs of labour were $26 per hour for tasks performed 'in-house' and $100 per hour for tasks that are outsourced: Ibid, 3.

244 Ibid, 6.

245 See App 4 of this Report.

Task	**Estimated weighted average cost per small business**	
	OSB	**Applied Economics**
1. Familiarisation with privacy legislation	$52.00	$31.00
2. Conduct a privacy audit	$89.00	$ 48.00
3. Develop a privacy plan	$133.50	$16.00
4. Amend existing business documentation	$100.00	$20.00
5. Train staff	$89.00	$34.00
6. Purchase of a filing cabinet	$299.00	$76.00
7. Purchase of a paper shredder	$79.00	
Total start-up cost	**$841.50**	**$225.00**
8. Handle customer complaints	$156.00	$120.00
9. Record keeping	$229.84	$112.00
10. Promulgate Privacy Policy	$499.00	$30.00
11. Update / review Privacy Policy	$39.00	$39.00
Total ongoing cost	**$923.84**	**$301.00**

39.136 An example of an alternative way to complete one of the compliance tasks concerned the publication of a Privacy Policy. The OSB assumed that the most streamlined approach to develop and publish a Privacy Policy would be to print 500 colour-printed flyers, at a cost of $499 per business, and distribute them on request.[246] Applied Economics, on the other hand, noted statistics published by the ABS showing that 40% of businesses with 5–15 employees have a website—and so could publish their Privacy Policy online at little or no cost. Further, Applied Economics estimated that 50% of businesses would create a Privacy Policy on their

246 Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007), 7–8.

computer and print out copies of the document at a cost of $0.50 per copy, resulting in a total cost of $10 per business. It also was estimated that only 5% of small businesses—for example, those dealing with government or large corporations—may consider it necessary to have a colour-printed Privacy Policy available at a cost of $499 per business. Accordingly, Applied Economics estimated that, to complete the task of developing and publishing a Privacy Policy, each business would incur a weighted average cost of only $30.

39.137 Similarly, the OSB assumed that every small business affected would have to engage a legal professional to amend their existing business documentation, such as emails, advertising and contracts, to include general information on their Privacy Policy, and in some instances, consent and disclosure clauses.[247] Applied Economics, on the other hand, noted that many small businesses (eg, convenience stores and beauty parlours) operate on the basis of informal (oral) contracts, and that advertising by many small businesses would not require the provision of general information on their Privacy Policy. Accordingly, Applied Economics estimated that only 20% of small businesses would consider it necessary to engage a legal professional to amend their business documentation and the weighted averaged cost per business would be $20.

39.138 Further, the OSB estimated that every small business operator would have to purchase a 'low range fully lockable filing cabinet' and a low range paper shredder at a combined cost of $378.[248] However, Applied Economics estimated that only 20% of small businesses would need to purchase these items, the rest already possessing them for other record-keeping purposes (such as tax and business planning). It was estimated, therefore, that the weighted average cost only would amount to $76 per business.

ALRC's view

39.139 After carefully reviewing stakeholder views, international experience, and the commissioned research, the ALRC concludes that the exemption for small business is neither necessary nor justifiable.

39.140 Associate Professor Moira Paterson has offered a counter to the argument that the requirement to comply with the *Privacy Act* constitutes a substantial compliance burden. She noted that the costs of compliance on businesses are likely to be significant only where businesses have poor record-keeping practices—citing evidence from Quebec that implementing data protection measures may in fact result in cost reduction or increased productivity due to improved information-handling practices.[249] Furthermore, Paterson observed that, in New Zealand,

247 Ibid, 5.
248 Ibid, 6–7.
249 M Paterson, 'Privacy Protection in Australia: The Need for an Effective Private Sector Regime' (1998) 26 *Federal Law Review* 372, 383, 399.

> the limited information available to date does not suggest that the cost of implementation has been a major problem. For example, the New Zealand Real Estate Institute commented in 1994 that, while the passing of the *Privacy Act 1993* (NZ) would have a considerable impact on the manner in which the industry might deal with personal information, it did not expect that there would be any significant cost of compliance; what was required was common sense and fair dealing.[250]

39.141 While cost of compliance with the *Privacy Act* is an important consideration, this factor alone does not provide a sufficient policy basis to support the small business exemption. The fact that no comparable overseas jurisdictions—including the United Kingdom, Canada and New Zealand—have an exemption for small businesses is indicative.

39.142 At present, potentially up to 94% of Australian businesses are exempt from the operation of the *Privacy Act*. Some stakeholders argued that exempting the majority of businesses from the operation of the Act is justified because small businesses pose a low risk to privacy. This assumption can be questioned on two grounds.

39.143 First, 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. Some small businesses, such as ISPs and debt collectors, hold large amounts of personal information. In addition, given the increasing use of technology by small businesses, the risk posed to privacy may not necessarily be low. In this regard, it should be noted that the OPC received a significant number of inquiries that related to this exemption.

39.144 Secondly, the fact that there are a considerable number of conditions that qualify the application of the exemption also suggests that the assumption that small businesses present a low risk to privacy is no longer valid. Under existing law, there already are seven categories of small businesses to which the small business exemption does not apply.[251] Some of these categories—namely, small businesses that operate or use residential tenancy databases, and those that are 'reporting entities' under the AML/CTF Act—were brought into the privacy regime after the enactment of the private sector provisions of the *Privacy Act* precisely because they raised significant privacy concerns.

39.145 The ALRC does not consider that further modifying the exemption is a sufficient response to the concerns raised in submissions and consultations. At whatever level the threshold for the exemption is set, the definition of 'small business' would be arbitrary, and consumers could not determine easily whether the exemption

---

250 Ibid, 399.

251 Generally speaking, as has been noted above, the exemption currently does not apply to health service providers; small businesses that trade in personal information; Australian Government contractors; small businesses that are related to larger businesses; persons who provide specified financial, gambling or bullion trading services; users and operators of residential tenancy databases; and small businesses that elect to 'opt in' to be covered by the *Privacy Act*.

applies to a particular business. In some cases, small businesses themselves may have problems understanding whether the exemption applies to their operations due to the various conditions that qualify the application of the exemption.

39.146 Further, the application of the small business exemption could have unintended consequences. For example, in the context of the Northern Territory Emergency Response, legislative provisions that were intended to protect Indigenous children in the Northern Territory from abuse raised concerns about the lack of safeguards against misuse of personal information, partly because small business operators are exempt from the operation of the *Privacy Act*.

39.147 The ALRC agrees with the 2005 Senate Committee privacy inquiry that regulating small businesses in some areas—such as telecommunications and debt collection—and not others, would add to the complexity of the privacy regime. The ALRC also notes that privacy concerns relating to small businesses are not confined to those that operate in particular industries. For example, given the highly sensitive nature of genetic information, small businesses that hold genetic information pose a particularly high risk to privacy, regardless of whether they provide a health service.[252] In 2006, the *Privacy Legislation Amendment Act 2006* (Cth) was passed to amend the definitions of 'health information' and 'sensitive information' in the *Privacy Act* to include genetic information about an individual.[253] Consequently, small businesses that hold genetic information and provide a health service no longer qualify for the small business exemption. Other small business that hold genetic information, however, still may be exempt from the operation of the *Privacy Act*. This would be the case where a small business meets all the other conditions that qualify the exemption.

39.148 Further, as discussed above, the removal of the small business exemption would bring Australia in line with other comparable countries—and would assist in achieving EU 'adequacy' status and facilitate trade with EU organisations.

39.149 Finally, the ALRC notes the submissions arguing that compliance costs on small businesses may be reduced by modifying the application of the privacy principles to small businesses, either through a code, a public interest determination by the OPC or specific exceptions to certain privacy principles. Modifying the application of the privacy principles to small businesses, however, would result in uneven privacy protection and a more complex privacy regime without addressing adequately concerns about unnecessary costs of compliance to small businesses.

---

252 See Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.102].

253 *Privacy Legislation Amendment Act 2006* (Cth) sch 2 cl 2. This amendment followed recommendations in Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003). The Australian Democrats unsuccessfully sought to remove the small business exemption, the political party exemption and the exemption for political acts and practices during parliamentary debate on the legislation: Commonwealth, *Parliamentary Debates*, Senate, 7 September 2006, 42 (N Stott Despoja).

Recommendation 39–1 The *Privacy Act* should be amended to remove the small business exemption by:

(a) deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and

(b) repealing ss 6D–6EA of the Act.

Minimising costs of compliance on small businesses

39.150 In DP 72, the ALRC acknowledged that removing the small business exemption would have compliance cost implications for small businesses. The ALRC expressed the view, however, that there are a number of ways that unnecessary compliance costs can be minimised, including by simplifying the *Privacy Act* and streamlining the privacy principles, and by assisting small businesses in understanding their regulatory rights and obligations.

Discussion Paper proposal

39.151 The ALRC proposed that, before the removal of the exemption, the OPC should provide dedicated assistance and support to small businesses, including: the establishment of a national helpline for small businesses; the development of educational materials; the provision of templates for Privacy Policies free of charge; and liaison with other government departments and industry bodies to provide educational programs targeted at small businesses.[254]

Submissions and consultations

39.152 A number of key stakeholders supported the proposal.[255] For example, Privacy NSW agreed that simplification of the *Privacy Act*, together with dedicated assistance by the OPC to small businesses, would help reduce compliance costs for small businesses.[256]

---

254 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 35–2.

255 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; National Legal Aid, *Submission PR 521*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 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; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

256 Privacy NSW, *Submission PR 468*, 14 December 2007.

39.153 The Government of South Australia suggested that the Privacy Commissioner should provide significant support through those state and territory authorities that support businesses. Further, it submitted that the OPC may need to provide different levels of support to particular industries in order to target different areas of privacy risk, or at least encourage industry cooperation to minimise the costs of compliance on small businesses that hold a small amount of personal information.[257]

39.154 The Australasian Compliance Institute submitted that there should be guidance notes for use by small businesses about how to reduce the risk of identity theft. It also suggested that the use of audit powers by the OPC on its own motion would be of particular assistance to small businesses as an educative tool to assist them in identifying areas for improvement within their privacy compliance framework.[258]

39.155 The OVPC submitted that a staggered introduction of privacy regulation, with a longer lead time for smaller businesses, could be considered as a means of assisting small businesses to prepare for compliance with the *Privacy Act*. It suggested that, in determining the different commencement dates for businesses of different sizes, a simpler, more transparent measurement should be adopted instead of the 'highly complex' annual turnover criterion. The OVPC suggested that a sliding scale of commencement dates could be based on the ABS categorisation of businesses in terms of the number of employees.[259]

39.156 While supportive of the ALRC's proposal, PIAC expressed concern that the proposal might be interpreted as making the removal of the small business exemption contingent upon the provision of support and advice by the OPC to small businesses. PIAC submitted that this could delay the removal of the exemption as well as other amendments to the *Privacy Act* indefinitely—which it regarded as inappropriate and unjustifiable. PIAC suggested that the removal of the exemption should take effect within a specific timeframe set in the legislation—for example, that the removal should take effect within three months of the enactment of the amended *Privacy Act*, and no more than 12 months after this time.[260]

39.157 Some stakeholders who opposed the removal of the small business exemption nevertheless supported the proposal that the OPC provide substantial assistance to small businesses.[261] For instance, the OPC stated that, if the small business exemption

---

257 Government of South Australia, *Submission PR 565*, 29 January 2008.

258 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

259 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. The ABS defines 'small businesses' as businesses that employ less than 20 people (except in the agricultural industry). Small businesses are categorised into three groups—'non-employing businesses', 'micro businesses' with between one and four employees, and businesses with between five and 19 employees: Australian Bureau of Statistics, *Characteristics of Small Businesses, Australia*, 8127.0 (2005), 101.

260 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

261 See, eg, Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007 (endorsed by Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007).

were to be removed, the ALRC's proposal is 'sensible and necessary to assist small business in understanding and meeting their obligations'. The OPC indicated that it should provide such support, as it is consistent with OPC's functions under s 27(d) and (e) of the *Privacy Act*. It noted, however, that fulfilling the additional requirements would have resource implications.[262]

39.158 The Arts Law Centre of Australia submitted that assistance to small businesses should be extended to not-for-profit organisations in the event that the exemption is removed. In addition, it was of the view that there 'should be support networks to assist people in adapting the templates to their needs' and funding for the provision of legal advice to small businesses in understanding their privacy responsibilities.[263]

39.159 Some business and industry groups argued that the provision of substantial advice and assistance from the OPC would not be sufficient to outweigh the adverse impact of the removal of the small business exemption.[264] For example, Australian Business Industrial submitted that, while such advice and assistance would be essential in the event that the small business exemption is removed, it would not be sufficient to counterbalance the compliance costs involved in the removal of the exemption:

> The difficulty in reaching and communicating with small business on these complex issues should not be underestimated. Small business are primarily concerned with the day-to-day running of their business, and often are unable to leave their workplace premises to attend training, or otherwise remain away from the 'front of shop' for any length of time, as they do not employ sufficient personnel to replace them.[265]

39.160 The Retail Motor Industry submitted that assistance and support from the OPC would not alleviate the concerns raised by small businesses that time would be taken away from their core business activities to ensure that their business is compliant with the UPPs.[266] COSBOA submitted that, while the initial implementation costs could be reduced by assistance from the OPC, the costs of compliance are 'largely on-going or unavoidable in nature' and would affect a large number of small businesses. In addition, it argued that there would be significant costs and resource implications for the OPC in providing such assistance and in regulating the small business sector.[267]

39.161 While recognising that dedicated assistance by the OPC would reduce the compliance burden on small businesses, CPA Australia Ltd made the point that the proposal did not recognise the cumulative effect that regulatory compliance has on

---

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

263 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007 (endorsed by Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007).

264 Australian Business Industrial, *Submission PR 444*, 10 December 2007; Australian Institute of Company Directors, *Submission PR 424*, 7 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; Real Estate Institute of Australia, *Submission PR 400*, 7 December 2007; Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

265 Australian Business Industrial, *Submission PR 444*, 10 December 2007.

266 See also Retail Motor Industry, *Submission PR 407*, 7 December 2007.

267 Council of Small Business of Australia, *Submission PR 389*, 6 December 2007.

businesses, and that the impact of regulation in one area should not be viewed in isolation from the effect of regulation on businesses in other areas.[268]

ALRC's view

39.162 The ALRC acknowledges and is sensitive to the fact that removal of the exemption will result in compliance costs for small businesses. The main thrust of this Report is to simplify and harmonise privacy laws and practices in Australia, and the ALRC makes a large number of recommendations aimed at reducing the complexity of the existing regime—in itself a substantial cause of the current costs of compliance. In Chapter 5, the ALRC recommends that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity, and that the privacy principles be streamlined. The simplification of the legislation should go some way towards reducing unnecessary costs of compliance to small businesses.

39.163 Another way to reduce compliance costs to small businesses is by assisting them in understanding their regulatory rights and obligations.[269] This can be achieved by the OPC providing dedicated assistance and support to small businesses, which should include:

- a special national helpline for small businesses, similar to the Australian Competition and Consumer Commission's small business helpline;[270]
- developing guidelines and other educational material;
- providing templates for Privacy Policies free of charge; and
- liaising with other government departments and industry bodies—such as the OSB, the Business Council of Australia and the ACCI—to provide educational programs targeted at small businesses.[271]

39.164 Such assistance should be in place before the removal of the exemption comes into effect. This will ensure that small businesses have sufficient time to understand their obligations under, and prepare for compliance with, the *Privacy Act* once the

---

268 CPA Australia, *Submission PR 476*, 14 December 2007.

269 Small Business Ministers Council, *Giving Small Business a Voice—Achieving Best Practice Consultation with Small Business (Endorsed Paper)* (2000) Australian Government Office of Small Business.

270 The helpline was established to assist small businesses in complying with the *Trade Practices Act 1974* (Cth): Australian Competition and Consumer Commission, *Easy Access for Small Business to Advice* (2005) <www.accc.gov.au/content/index.phtml/itemId/718924> at 23 April 2008.

271 It should be noted that, currently, the OPC provides several plain English resources to assist small businesses in understanding whether they are covered by the *Privacy Act* and, if so, their obligations under the Act, including, eg, Office of the Privacy Commissioner, *A Snapshot of the Privacy Act for Small Business (Updated with Minor Amendments 27 November 2007)* (2007); Office of the Privacy Commissioner, *A Privacy Checklist for Small Business (Updated with Minor Amendments 27 November 2007)* (2007); Office of the Privacy Commissioner, *A Guide to Privacy for Small Business (Updated with Minor Amendments 27 November 2007)* (2007).

exemption is removed. Finally, it is essential that the OPC is resourced adequately to assist small businesses.

39.165 The ALRC acknowledges the concern that making the removal of the small business exemption contingent on assistance being provided by the OPC may delay indefinitely the removal of the exemption. While no recommendation is made for a fixed timeframe, the ALRC agrees that the removal of the exemption should come into force within a year from the enactment of the amended *Privacy Act*.

Recommendation 39–2 Before the removal of the small business exemption from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by:

(a) establishing a national hotline to assist small businesses in complying with the Act;

(b) developing educational materials—including guidelines, information sheets, fact sheets and checklists—on the requirements under the Act;

(c) developing and publishing templates for small businesses to assist in preparing Privacy Policies, to be available electronically and in hard copy free of charge; and

(d) liaising with other Australian Government agencies, state and territory authorities and representative industry bodies to conduct programs to promote an understanding of the privacy principles.

40. Employee Records Exemption

Contents

Introduction

40.1 The *Privacy Act 1988* (Cth) defines an 'employee record' as a record of personal information relating to the employment of the employee.[1] Under the Act, the handling of an 'employee record' by a public sector employer is treated differently from the handling of such a record by a private sector employer. For Australian Government agencies, the *Privacy Act* does not distinguish between the handling of employee records and the handling of other 'personal information' as defined in the Act. Accordingly, an agency must handle employee records in compliance with the Act.

40.2 In contrast, a private sector organisation that is or was an employer of an individual is exempt from the operation of the *Privacy Act* where its act or practice is related directly to: the employment relationship between the organisation and the individual; and an employee record held by the organisation.[2] This exemption usually is referred to as the 'employee records exemption'.

40.3 This chapter examines whether the employee records exemption should remain. The ALRC concludes that there is no sound policy justification for retaining the employee records exemption and recommends its removal. In light of the concerns raised about the application of the *Privacy Act* to employee records, the ALRC also recommends that the Office of the Privacy Commissioner (OPC) should develop and publish guidance to assist employers to comply with the Act.

40.4 This chapter also considers whether evaluative materials, such as employment references, should be excluded from the application of the *Privacy Act*, and concludes that they should not be excluded given that the model Unified Privacy Principles (UPPs) are sufficiently flexible to accommodate the competing interests.

40.5 Finally, the chapter discusses whether privacy protection of employee records should be located in the *Privacy Act* or in other legislation. The ALRC concludes that privacy protection of employee records should be located in the *Privacy Act* to ensure maximum coverage of agencies and organisations and to promote consistency.[3]

---

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

2 Ibid ss 7(1)(ee), 7B(3).

3 The chapter does not deal with other workplace privacy issues, such as workplace surveillance (including email and internet monitoring), covert surveillance practices, surveillance and monitoring employees outside of work, and genetic testing in the workplace. As discussed in Ch 1, these issues have been considered in a report by the Victorian Law Reform Commission into workplace privacy: Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005). The VLRC report is under consideration by the Standing Committee of Attorneys-General.

Background

Current law

40.6 Section 6 of the *Privacy Act* defines 'employee record' to mean a record of personal information relating to the employment of the employee. Examples of such personal information include health information about the employee, and personal information about:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee;

(c) the terms and conditions of employment of the employee;

(d) the employee's personal and emergency contact details;

(e) the employee's performance or conduct;

(f) the employee's hours of employment;

(g) the employee's salary or wages;

(h) the employee's membership of a professional or trade association;

(i) the employee's trade union membership;

(j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;

(k) the employee's taxation, banking or superannuation affairs.[4]

40.7 Acts and practices of an organisation are exempt from the operation of the *Privacy Act* if they are related directly to a current or former employment relationship.[5] Accordingly, the exemption does not apply to: acts and practices of an employer that are beyond the scope of the employment relationship;[6] the handling of personal information about unsuccessful job applicants;[7] and the handling of employee records by contractors and subcontractors to the employer.[8]

---

4 *Privacy Act 1988* (Cth) s 6(1). This list was not intended to be exhaustive: Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [22]. Some information held by employers relating to individual employees—for example, emails received by an employee from third parties—may not necessarily be an 'employee record': Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 3.

5 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(3).

6 For example, employers cannot sell a list of employees for marketing purposes: Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 3–4. See also *C v Commonwealth Agency* [2005] PrivCmrA 3, in which the Privacy Commissioner determined that the disclosure of an employee record by an employer to the employer's legal counsel in connection with proceedings that did not concern the employee was not an act that was related directly to the employment relationship, and therefore did not fall within the employee records exemption.

7 Once an employment relationship is established, however, records of pre-employment checks on the individual employee become exempt: Office of the Privacy Commissioner, *Coverage of and Exemptions*

40.8 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) stated that:

> The act or practice must be directly related to a current or former employer relationship so as to ensure that employers cannot use 'employee records' for commercial purposes unrelated to the employment context.[9]

40.9 The reason given for the employee records exemption was that:

> While this type of personal information is deserving of privacy protection, it is the government's view that such protection is more properly a matter for workplace relations legislation.[10]

40.10 The website of the Attorney-General's Department (AGD) indicates that:

> The potential also exists for Commonwealth privacy regulation of employee records to have unintended consequences where it intersects with State and Territory laws dealing with employee records.[11]

40.11 Currently, there is little privacy protection for private sector employees under the federal workplace relations regime. Regulations 19.18 and 19.19 of the *Workplace Relations Regulations 2006* (Cth) allow employees to access certain records. This, however, only applies to records about conditions under which employees are hired, overtime and reasonable additional hours worked, remuneration, leave, superannuation contributions and termination.[12] It does not include other personal information that falls within the definition of 'employee record' in the *Privacy Act*, for example, employees' health information, or their taxation or banking affairs. The regulations only require employers to maintain, provide access to, and correct records for official inspection for auditing purposes, rather than to protect the privacy of those records.[13] In addition, under the *Workplace Relations Act 1996* (Cth), privacy protection is not a term that may be included in awards. As a consequence, the Australian Industrial Relations Commission does not have jurisdiction to make an award about privacy.[14]

---

from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007), Information Sheet 12 (2001), 3.

8 Ibid, 4. The Office of the Privacy Commissioner has stated that 'in many circumstances, the employee records exemption may not apply to organisations that provide recruitment, human resource management services, medical, training or superannuation services under contract to an employer': Office of the Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 27 November 2007)*, Information Sheet 12 (2001), 3–4.

9 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [109].

10 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15752. See also Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 4, [109].

11 Australian Government Attorney-General's Department, *Employee Records* (2000) <www.ag.gov.au> at 8 May 2008.

12 *Workplace Relations Regulations 2006* (Cth) regs 19.7–19.14.

13 Ibid ch 2, pt 2, divs 2–3. See also M Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169, 175.

14 *Workplace Relations Act 1996* (Cth) s 513. See also M Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169, 175.

40.12 At the state level, legislation only requires employers to maintain, and in most cases, provide an employee with access to, certain basic records about employees, such as time and wage records.[15] At common law, an employer is under a duty of mutual trust and confidence not to 'conduct itself in a manner likely to destroy or seriously damage the relationship of confidence and trust between employer and employee'.[16] Professor Margaret Otlowski argues that,

> existing contractual and equitable principles for maintaining confidentiality … may offer some protection to employees. However, such actions are in practice, costly to pursue (involving private litigation in the civil courts) and not easy to establish.[17]

40.13 There is no exemption for the handling of employee records by agencies under the *Privacy Act*. Australian Government and ACT agencies, therefore, are required to comply with the Information Privacy Principles (IPPs) when dealing with employee records.[18] Privacy legislation in New South Wales, Victoria and the Northern Territory also applies to employee records of public sector employees.[19] In Tasmania, public sector bodies, councils, the University of Tasmania, prescribed bodies, and contractors to these entities have to comply with the personal information protection principles under the *Personal Information Protection Act 2004* (Tas) in dealing with employee information, subject to certain exceptions.[20] The Victorian *Health Records Act 2001* also regulates the handling of health information, including information contained in employee records, by public and private sector entities.

40.14 A number of overseas jurisdictions—including the United Kingdom, Ireland, New Zealand and Hong Kong—do not exempt employee records from the operation of their privacy or data protection legislation. They do, however, commonly provide for exceptions to their data protection principles when dealing with personal information for the purposes of recruitment, appointments and contracts for the provision of services.[21] Some overseas privacy legislation also provides an exception for personal

---

15 See, eg, *Industrial Relations Act 1996* (NSW) s 129; *Industrial Relations Act 1999* (Qld) ch 11 pt 1; *Minimum Conditions of Employment Act 1993* (WA) pt 6; *Industrial Relations Act 1984* (Tas) s 75. The New South Wales legislation does not provide for the right of an employee to access his or her records.

16 *Malik v Bank of Credit & Commerce International SA (in liq)* [1998] AC 20 45–46; *Blaikie v South Australian Superannuation Board* (1995) 65 SASR 85; *Brackenridge v Toyota Motor Corporation Australia Ltd* (1996) 142 ALR 99; *Burazin v Blacktown City Guardian Pty Ltd* (1996) 142 ALR 144; *Jager v Australian National Hotels Pty Ltd* (1998) 7 Tas R 437.

17 M Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169, 175.

18 A slightly amended version of the *Privacy Act 1988* (Cth) applies to ACT government agencies: *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth) s 23.

19 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic); *Information Act 2002* (NT).

20 *Personal Information Protection Act 2004* (Tas) ss 3 (definition of 'personal information custodian'), 10, sch 1, cl 2(1)(i)–(j).

21 See, eg, *Data Protection Act 1998* (UK) sch 7, cls 3, 4; *Data Protection Act 1988* (Ireland) s 4(13); *Personal Data (Privacy) Ordinance* (Hong Kong) s 55.

references relevant to an individual's suitability for employment or appointment to office.[22]

40.15 There is no general exemption for employee records under the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines), the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament or the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[23]

40.16 In 2001, the Article 29 Data Protection Working Party of the European Commission released its advisory opinion on the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Working Party stated that employee records often contain sensitive information and saw no reason to exclude them from the protection provided for sensitive information by National Privacy Principle (NPP) 10. Further, the Working Party observed that the exemption allows information about previous employees to be collected and disclosed to a third party (eg, a future employer) without the employee being informed.[24]

40.17 For the period from 21 December 2001 to 31 January 2005, the OPC indicated that 12% of all the NPP complaints closed by the Office as outside of its jurisdiction concerned the employee records exemption.[25] In 2005–06, the OPC received 2,000 inquiries concerning exemptions, of which 43% related to the employee records exemption.[26]

---

22 See, eg, *Data Protection Act 1998* (UK) sch 7, cl 1; *Privacy Act 1993* (NZ) s 29(1)(b); *Personal Data (Privacy) Ordinance* (Hong Kong) s 56.

23 Article 8(2)(b) of the EU Directive, however, provides that processing of certain sensitive personal data may be allowed if it is 'necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards': European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 8(2)(b). The APEC Privacy Framework provides that when using personal information for employment purposes, employers may not need to comply with the principle that individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information in certain situations: Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [20].

24 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 4. One commentator suggests that this misstates the position in that the exemption does not allow a past employer to forward information to a prospective employer without informing the employee: P Ford, 'Implementing the EC Directive on Data Protection—An Outside Perspective' (2003) 9 *Privacy Law & Policy Reporter* 141, 145.

25 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

26 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 27. There were no similar statistics in the OPC's most recent annual report: see Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007).

Previous inquiries

40.18 In 2000, the House of Representatives Standing Committee on Legal and Constitutional Affairs concluded an inquiry into the Privacy Amendment (Private Sector) Bill (2000 House of Representatives Committee inquiry). The 2000 House of Representatives Committee inquiry was not satisfied that existing workplace relations legislation provided adequate protection for the privacy of private sector employee records, and expressed 'grave concerns' about the exemption.[27]

40.19 The 2000 House of Representatives Committee inquiry stated that employees are in need of privacy protection because employers frequently hold a large amount of information about their employees, some of which can be extremely sensitive—such as health information, genetic test results, financial details and results of psychological testing conducted before employment. The inquiry acknowledged that there are competing considerations and that employers should be able to disclose some information to future employers, such as confidential references. It considered that a distinction could be drawn in the nature, but not the sensitivity, of the information that may be held in employee records. It was the inquiry's view that employees are entitled to expect confidentiality of their workplace records given that they have little choice about providing information to their employers.[28]

40.20 A particular issue was whether the health information of employees should be covered by the *Privacy Act*. The 2000 House of Representatives Committee inquiry strongly objected to the inclusion of 'health information' in the definition of 'employee record'. It also noted that this was inconsistent with the more specific protection given to health information and sensitive information elsewhere in the Privacy Amendment (Private Sector) Bill.[29]

40.21 In the opinion of the 2000 House of Representative Committee inquiry, most employee records should be given the protection of the NPPs. The inquiry therefore recommended that the definition of 'employee records' should be revised to exempt only a limited list of personal information from the operation of the *Privacy Act*. These included a record of personal information relating to: the engagement, training, disciplining or resignation of the employee; the termination of the employment of the employee; and the employee's performance or conduct.[30]

40.22 In rejecting the recommendations by the 2000 House of Representatives Committee inquiry, the Australian Government stated that:

---

27 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.29].
28 Ibid, [3.30]–[3.33].
29 Ibid, [3.37].
30 Ibid, [3.28], recs 5–7.

> The regulation of employee records is an area that intersects with a number of State and Territory laws on workplace relations, minimum employment conditions, workers' compensation and occupational health and safety, some of which already include provisions protecting the privacy of employee records. The Government considers that to attempt to deal with employee records in the [Privacy Amendment (Private Sector)] Bill might result in an unacceptable level of interference with those State and Territory laws, and a confusing mosaic of obligations.[31]

40.23 In their 2003 report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council recommended that the *Privacy Act* should be extended to cover genetic information contained in employee records.[32] The ALRC and AHEC further recommended that the forthcoming inter-departmental review of employee privacy by the AGD and the Department of Employment and Workplace Relations (DEWR) should consider whether the *Privacy Act* should be amended to cover other forms of health information contained in employee records.[33]

40.24 In February 2004, the AGD and DEWR released a discussion paper on the privacy of employee records.[34] The discussion paper examined the current level of privacy protection for employee records under existing federal, state and territory laws. It also considered some privacy concerns about employee records and suggested options for enhancing privacy. These options included: retaining the exemption; abolishing or modifying the exemption; establishing specific employee records privacy principles; and protecting employee records in workplace relations legislation.[35] No final recommendations were made after the release of the discussion paper.

40.25 In its report, *Workplace Privacy—Final Report* (2005), the Victorian Law Reform Commission (VLRC) commented that 'the operation of the employee records

---

31 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007. During the OPC's review of the privacy sector provisions of the *Privacy Act*, a number of submissions and consultations commented on the employee records exemption, despite the fact that it was expressly excluded from the terms of reference for the Review: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 285.

32 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 34–1.

33 Ibid, Rec 34–2.

34 Australian Government Attorney-General's Department and Australian Government Department of Employment and Workplace Relations, *Employee Records Privacy: A Discussion Paper on Information Privacy and Employee Records* (2004).

35 Ibid, [4.15]–[4.42]. The review of the *Privacy Act* by the Senate Legal and Constitutional References Committee expressed disappointment at the slow progress of the AGD and DEWR review, and considered the finalisation and release of the results of the review a matter of urgency: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.35].

exemption leaves a significant gap in the privacy protection of workers' personal information'.[36]

40.26 In April 2006, the Standing Committee of Attorneys-General agreed to establish a working group to advise ministers on options for improving consistency in privacy regulation, including workplace privacy.[37] In its response to the 2006 report by the Productivity Commission's Taskforce on Reducing Regulatory Burdens on Business, the Australian Government stated that the working group would liaise with—and not duplicate the work of—the ALRC in this area.[38]

40.27 In November 2006, the House of Representatives Standing Committee on Legal and Constitutional Affairs released a report on the harmonisation of legal systems within Australia and between Australia and New Zealand. In its report, the Committee recommended that 'the Australian Government highlight the issue of regulatory inconsistency in privacy regulation, including in the area of workplace privacy regulation', in its submissions to the current Inquiry.[39]

EU adequacy and the APEC Privacy Framework

40.28 The European Union (EU) has not granted Australia 'adequacy status' under the EU Directive.[40] The OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) noted that there were continuing negotiations with the European Commission regarding the adequacy of the *Privacy Act*, especially in relation to the small business and employee records exemptions.[41] The OPC Review concluded that, although there was 'no evidence of a broad business push' for achieving EU adequacy, there may be long-term benefits for Australia in achieving such adequacy. The OPC Review therefore recommended that the Australian Government continue to work with the EU on this issue.[42] The Australian Government agreed with this recommendation.[43]

---

36 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [1.19].

37 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 26.

38 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

39 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Harmonisation of Legal Systems within Australia and between Australia and New Zealand* (2006), rec 25.

40 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 14(b).

41 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

42 Ibid, rec 17.

43 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 4.

40.29 In addition, the OPC Review noted that the increase in cross-border data flows makes implementation of international privacy frameworks important. The OPC, therefore, also recommended that the Australian Government continue to work within APEC to implement the APEC Privacy Framework.[44]

40.30 In its inquiry into the *Privacy Act* in 2005, the Senate Legal and Constitutional References Committee (2005 Senate Committee privacy inquiry) noted with concern that current workplace relations legislation does not protect workplace privacy adequately, and recommended that this Inquiry examine the precise mechanisms under the *Privacy Act* to protect employee records.[45] It also recommended that the current Inquiry investigate possible measures that could assist Australia in achieving EU adequacy.[46] The Australian Government disagreed with this recommendation, on the basis that 'international negotiations are a matter for the Australian Government and negotiations with the European Union are ongoing'.[47] The issue of EU adequacy is discussed further in Chapter 31.

Discussion Paper proposal

40.31 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC considered whether the employee records exemption should be removed. The ALRC noted that employee records may contain a significant amount of personal information about employees, including sensitive information. There is a real potential for individuals to be harmed if employees' personal information is used or disclosed inappropriately. The ALRC stated that the lack of adequate privacy protection for employee records in the private sector is of particular concern because employees may be under economic pressure to provide personal information to their employers.

40.32 The ALRC's preliminary view was that there is no sound policy reason why privacy protection for employee records is available to public sector employees but not private sector employees. In addition, treating employees' personal information differently from other personal information also cannot be justified. The ALRC proposed, therefore, that the employee records exemption should be removed.[48]

40.33 Stakeholders were divided on the ALRC's proposal to remove the employee records exemption. Most employers and employer groups were in favour of retaining

---

44 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 17.

45 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.36]–[7.38]; recs 13, 14.

46 Ibid, rec 16.

47 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), 5.

48 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 36–1.

the exemption,[49] while privacy authorities, privacy advocates, an employee group and others supported removing the exemption.[50] A range of reasons for removing and retaining the exemption were advanced, which are discussed in detail below.

Arguments for removing the exemption

Lack of privacy protection for employee records

40.34 Stakeholders noted that employers may hold sensitive personal information about their employees, such as health or financial information;[51] criminal convictions; and the results of pre-employment psychological testing.[52] Employees may be under economic pressure to provide personal information to their employers. This means that they have no effective choice but to provide such information.[53]

> In many cases information is collected from employees as a condition of their employment; for example, health information, criminal charges or convictions and financial matters such as bankruptcy or garnishee of wages. The exemption allows

---

49 See, eg, GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Australian Information Industry Association, *Submission PR 410*, 7 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007 (supported by Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007); IBM Australia, *Submission PR 405*, 7 December 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007 (endorsed by the National Australia Bank, *Submission PR 408*, 7 December 2007). Three Australian Government departments also opposed the proposal: New South Wales Government Department of Health, *Submission PR 458*, 11 December 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

50 See, eg, Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Lawyers Alliance, *Submission PR 528*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 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; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 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; Australia Post, *Submission PR 445*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007; ACTU, *Submission PR 155*, 31 January 2007.

51 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; ACTU, *Submission PR 155*, 31 January 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.

52 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

53 Ibid; Privacy NSW, *Submission PR 468*, 14 December 2007; ACTU, *Submission PR 155*, 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

> this information to be disclosed to others in circumstances which could be very damaging to the individual.[54]

40.35 Concern was expressed about the existing lack of privacy protection for employee records. National Legal Aid submitted that the broad definition of 'employee records' in the *Privacy Act* means that employers may accumulate a considerable range of personal information about employees covering sensitive matters, such as health, drug tests and disciplinary issues, without being accountable for the way the information is handled.[55] The Centre for Law and Genetics suggested that there was a real potential for individuals to be harmed if such sensitive personal information was used or disclosed inappropriately.[56]

40.36 Several stakeholders raised particular concerns about the privacy of employees' health information.[57] For example, the Victorian Office of the Health Services Commissioner stated that it has received many inquiries and complaints from employees about their health information being inappropriately collected or disclosed, or not being stored securely.[58] The Mental Health Legal Centre expressed concern about the release of information about a person's mental health to prospective employers, which could affect their future job options. It noted that such information could include the fact that a potential employee was found not guilty on the grounds of mental impairment.[59] One stakeholder who opposed removing the employee records exemption indicated that it would support the exclusion of health information from the exemption, given the sensitive nature of health information.[60]

40.37 Some stakeholders noted gaps in the protection of employees' privacy in legislation[61] and, in particular, the limited protection provided by the workplace relations legislation.[62] For example, the OPC observed that, in the Second Reading Speech for the Privacy (Private Sector) Amendment Bill, the then Attorney-General stated that employee records were 'deserving of privacy protection' but that such

---

54 ACTU, *Submission PR 155,* 31 January 2007.

55 National Legal Aid, *Submission PR 521,* 21 December 2007. See also H Fisher, *Submission PR 582,* 31 March 2008.

56 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

57 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Mental Health Legal Centre Inc, *Submission PR 184,* 1 February 2007; 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.

58 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

59 Mental Health Legal Centre Inc, *Submission PR 184,* 1 February 2007.

60 Confidential, *Submission PR 529,* 21 December 2007.

61 Privacy NSW, *Submission PR 468,* 14 December 2007; Law Institute of Victoria, *Submission PR 200,* 21 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; ACTU, *Submission PR 155,* 31 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

62 Privacy NSW, *Submission PR 468,* 14 December 2007; Law Institute of Victoria, *Submission PR 200,* 21 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

protection was 'more properly a matter for workplace relations legislation'.[63] The OPC noted that, despite this statement, workplace relations legislation has not been amended to enhance the privacy protection of employee records.[64] Privacy NSW submitted that:

> while the employee records exemption … was predicated on the idea that employee records would be protected under workplace relations legislation, the failure by the federal government to do so has left private sector employees in an information privacy void.[65]

40.38 National Legal Aid noted that access to employee records under the *Workplace Relations Act* was limited, and submitted that employees should have better access to their employment records.[66] In contrast, other stakeholders submitted that granting employees the right to access personal information in their personnel files could be problematic. One stakeholder submitted that allowing employees to access security-sensitive information contained in personnel files collected during background checks on the employee could jeopardise the security of the workplace.[67] The Australian Bankers' Association Inc (ABA) submitted that certain categories of information in a workplace context should be excluded from the access regime under the *Privacy Act*, including investigation and management of workplace issues, and industrial relations activities where the information involved is not protected by a duty of confidence. The ABA argued that, where these categories of information are not excluded, employers may utilise external avenues to resolve issues.[68]

40.39 Some stakeholders contended that there is sufficient privacy protection for employees under existing federal and state laws, including laws concerning workplace relations, equal employment opportunity, anti-discrimination, occupational health and safety (OH&S), workers compensation, contracts and unfair dismissal.[69] The Australian Chamber of Commerce and Industry (ACCI) also suggested that, under the *Workplace Relations Act* and similar state and territory legislation, the keeping of certain employee records is regulated by a well-resourced inspectorate and employers could be subject to substantial penalties for non-compliance.[70]

---

63 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; citing Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15752.

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

65 Privacy NSW, *Submission PR 468*, 14 December 2007.

66 National Legal Aid, *Submission PR 521,* 21 December 2007. See also H Fisher, *Submission PR 582,* 31 March 2008.

67 Confidential, *Submission PR 536*, 21 December 2007.

68 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008.

69 Confidential, *Submission PR 536,* 21 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494,* 19 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007.

70 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

40.40 Some stakeholders submitted that employers already handle employee records with care.[71] For example, the ABA advised that 'each member bank has its own policies and practices in relation to the keeping, maintenance and control of and access to its employees' records'.[72] UNITED Medical Protection stated that their human resources department operates on the basis of preserving employees' confidentiality.[73] The ACCI submitted that the existence of the employee records exemption does not mean that employers would not have adequate safeguards in place to protect employee records from misuse or exploitation.[74]

40.41 Some stakeholders noted that the employee records exemption is limited in its scope,[75] and strongly objected to narrowing the scope of the exemption.[76] DEWR stated that limiting the scope of the exemption,

> for instance, by retaining some of the NPPs for employee records or restricting the exemption by excluding sensitive information from it, would only contribute to the complexity of the privacy framework.[77]

40.42 The ACCI noted that the exemption was confined to records of current or former employees that were related directly to the employment relationship. It submitted that, where the exemption does not apply, any misuse of personal information could have two adverse consequences for employers. First, it potentially would expose the employer to common law actions, such as breach of the implied duty of mutual trust and confidence, the tort of negligence and breach of contract. Secondly, handling personal information inappropriately could damage the reputation and goodwill of a business. These two potential consequences helped to ensure that businesses handle personal information about employees appropriately.[78]

Level of complaint

40.43 A significant number of complaints closed by the OPC as falling outside its jurisdiction concern the employee records exemption.[79] Stakeholders also submitted

---

71 Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007 (endorsed by the National Australia Bank, *Submission PR 408*, 7 December 2007); Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; UNITED Medical Protection, *Submission PR 118*, 15 January 2007.

72 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007 (endorsed by the National Australia Bank, *Submission PR 408*, 7 December 2007).

73 UNITED Medical Protection, *Submission PR 118*, 15 January 2007.

74 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.

75 Optus, *Submission PR 532*, 21 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

76 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.

77 Ibid.

78 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

79 See, eg, Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

that experience in other jurisdictions shows that employees need to exercise privacy rights.[80] Privacy NSW receives a significant number of complaints by, and inquiries from, employees against public sector agencies in New South Wales and stated that:

> 10% of internal review applications conducted in 2005–06 related to employee records. In addition 4.5% of complaints and 5.5% of enquiries received by [Privacy NSW] in the same year related to employee records. From this it is clear that employees in NSW have concerns about the way their personal information has been dealt with by their employers.[81]

40.44 The Cyberspace Law and Policy Centre stated that the high number of complaints concerning employee records were unsurprising because the consequences of misuse could be serious and far-reaching in an employment context.[82] Individuals expressed concern, for example, about: résumés containing personal information, including tax file numbers, being misused;[83] employers making inquiries about their employees without the employees' permission;[84] and recruitment companies collecting information from previous employers.[85]

40.45 Other stakeholders maintained that there is no evidence of any systemic problems or detriments caused by the exemption that justifies its removal.[86] For example, DEWR stated that submissions to the AGD and DEWR's discussion paper on employee records privacy 'did not disclose any significant detriment caused by the employee records exemption that warranted changing the status quo and imposing additional compliance costs on business'.[87]

40.46 The ACCI submitted that the onus should be on those parties who wished to alter the status quo to provide evidence that the exemption should be removed. The ACCI did not consider that the number of inquiries made to the OPC constitutes sufficient evidence that employers are handling personal information about employees

---

80 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

81 Privacy NSW, *Submission PR 468*, 14 December 2007.

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

83 Confidential, *Submission PR 535*, 21 December 2007.

84 Confidential, *Submission PR 374*, 5 December 2007.

85 D Collins, *Submission PR 369*, 4 December 2007.

86 Optus, *Submission PR 532*, 21 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Abacus–Australian Mutuals, *Submission PR 174*, 6 February 2007; UNITED Medical Protection, *Submission PR 118*, 15 January 2007.

87 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007, referring to Australian Government Attorney-General's Department and Australian Government Department of Employment and Workplace Relations, *Employee Records Privacy: A Discussion Paper on Information Privacy and Employee Records* (2004).

inappropriately.[88] The Australian Industry Group (AIG) and the Australian Electrical and Electronic Manufacturers' Association (AEEMA) submitted that mandatory regulation only should be considered if there is widespread abuse and if other measures such as education are ineffective.[89] Telstra submitted that, if there are concerns that employee records have not been handled properly, workplace relations legislation should be reformed to address those concerns in a manner that is consistent with other employment-related legislation.[90]

Differential treatment between public and private sectors

40.47 Stakeholders expressed concern that the *Privacy Act* protects the records of public sector employees but not those employed in the private sector.[91] This differential treatment is highlighted by the handling of employee records by Australian Government agencies that are subject to the IPPs in their non-commercial activities and the NPPs in their commercial activities. Australian Post, for example, noted that:

> staff who are employed by Australian Post in connection with its commercial activities do not have the same rights of access to their employment records under the law as their colleagues who are employed by the Corporation with its non-commercial activities.[92]

40.48 Stakeholders observed that it seems wrong for the privacy rights of public sector employees to be different from those in the private sector.[93] The Australian Council of Trade Unions stated that:

> The moral case for employers being required to respect the confidentiality of information acquired by them about their employees in the course of the latter's employment seems unassailable. It is consistent with the common law duty of trust and confidence which courts have found employers to owe their employees, including in respect of information provided by employees.[94]

40.49 The Office of the Victorian Privacy Commissioner (OVPC) highlighted that, 'besides simple equity', the repeal of the employee records exemption is desirable because

> Australia's workforce is increasingly mobile, and an agile economy should encourage that mobility. Many employees will operate in the private sector and as contracted service providers to government in outsourcing arrangements. Privatisation may take a workforce from a public sector to a private sector environment. The human

---

88 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

89 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007.

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

91 Government of Victoria, *Submission PR 288*, 26 April 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; Australia Post, *Submission PR 78*, 10 January 2007.

92 Australia Post, *Submission PR 78*, 10 January 2007.

93 ACTU, *Submission PR 155*, 31 January 2007; AAMI, *Submission PR 147*, 29 January 2007.

94 ACTU, *Submission PR 155*, 31 January 2007.

> resources management aspects of these kinds of factors, in practice, are likely to be simplified if basic privacy protection standards apply consistently across all sectors and across borders.[95]

40.50 Other stakeholders did not consider that the differential treatment of employee records in the public and private sectors is a sufficient reason for removing the employee records exemption.[96] For example, Australian Business Industrial submitted that:

> private industry and public sector agencies have very different stakeholders, objectives and operative environments, and it is neither appropriate nor fair to compare or expect consistency for the sake of consistency.[97]

Regulatory inconsistency and fragmentation

40.51 Some stakeholders submitted that retaining the employee records exemption likely would lead to further fragmentation of privacy regulation in states that have enacted legislation regulating the area of workplace privacy.[98] These stakeholders were of the view that, in the interests of national consistency, the *Privacy Act* should apply to the personal information of employees in place of existing state legislation in this area.[99]

40.52 Stakeholders submitted that removing the employee records exemption would help promote national consistency in privacy regulation.[100] The OPC noted, in particular, that sensitive information—including that held by employers about their employees—should be covered fully by the *Privacy Act*.[101]

40.53 The OVPC submitted that removing the exemption also would promote consistency among federal and state privacy commissioners and other relevant

---

95 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007. See also Government of Victoria, *Submission PR 288,* 26 April 2007.

96 Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007; Australian Business Industrial, *Submission PR 444,* 10 December 2007; Retail Motor Industry, *Submission PR 407,* 7 December 2007 (endorsed by Motor Traders Association of NSW, *Submission PR 429,* 10 December 2007).

97 Australian Business Industrial, *Submission PR 444,* 10 December 2007.

98 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

99 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

100 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Queensland Government, *Submission PR 490,* 19 December 2007.

101 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007. The OPC argued, however, that the employee records held by small business operators should remain exempt because there were 'clear and compelling' policy reasons for retaining the small business exemption. The small business exemption is discussed in Ch 39.

authorities in dealing with employee records matters.[102] The Queensland Government stated that the ALRC's proposal to remove the employee records exemption, together with the proposed removal of the small business exemption, would address both a gap in privacy coverage and ensure national consistency.[103]

40.54 In contrast, other stakeholders expressed concern that removing the employee records exemption would create another layer of regulation.[104] The Australian Retailers Association, for example, submitted that 'abolishing the employee records exemption within the *Privacy Act* only would increase the complexity of the Act and cause confusion'.[105] The ACCI stated that subjecting employers to the *Privacy Act* in their handling of employee records would add to existing multiple regulation in the employment area, including OH&S, workers compensation, equal employment opportunity and unfair dismissal.[106] The ACCI also expressed concern that:

> State and Territory privacy legislation is not consistent with the Commonwealth Act and ultimately leads to uncertainty. ACCI advocates that an employee records exemption is so fundamental that it should not only be retained, but also applied at the State and Territory level.[107]

40.55 The Motor Traders Association of NSW submitted that the complexity of privacy regulation of health information in Australia would cause problems for employers within the motor vehicle industry involving, for example, pre-employment medical examinations, medical certificates and other medical records, drug and alcohol testing, communicable diseases in the workplace, and the transfer of employees' health records where businesses are transferred. The problems could include:

- 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 (both employer and employees) about their rights and obligations.[108]

International standards and overseas jurisdictions

40.56 Some stakeholders submitted that compatibility with international standards and overseas jurisdictions should be a factor in considering whether the employee records

---

102 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
103 Queensland Government, *Submission PR 490*, 19 December 2007.
104 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007.
105 Australian Retailers Association, *Submission PR 131*, 18 January 2007.
106 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.
107 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007. The ACCI also noted that, given changes to the workplace relations system brought about by the passage of the 'Work Choices' legislation and further change subsequent to the change of government in the November 2007 election, reform of the employee records exemption should not be considered at this time.
108 Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007.

exemption should remain.[109] The New Zealand Privacy Commissioner noted the desirability of trans-Tasman compatibility, which could be facilitated, for example, by 'a seamless application of privacy protections for the information of prospective employees applying for work in the other country', or 'former employees after they return home'.[110]

40.57 Other stakeholders noted that the employee records exemption is an obstacle to the EU determining that Australia's privacy laws are adequate for the purposes of cross-border data flows under the EU Directive.[111] Professor Graeme Greenleaf, Nigel Waters and Associate Professor Lee Bygrave noted that the Article 29 Working Party has expressed concern that human resource data often were traded across borders and often contained sensitive information. Although there were no empirical data on the quantity and nature of information flows from Europe to Australia,

> there can be little doubt that personal data *are* being transferred along this channel and that at least some of these relate to current or past employment matters, and are, in addition, sensitive.[112]

40.58 The OVPC submitted that the removal of the employee records exemption would increase the likelihood of Australia achieving EU adequacy.[113] The Public Interest Advocacy Centre (PIAC) submitted that the employee records exemption also was likely to be an obstacle to any assessments of adequacy under the privacy law of other countries and other privacy instruments, such as the APEC Privacy Framework.[114]

40.59 While supportive of the ALRC's proposal to remove the employee records exemption, the Australasian Compliance Institute stated that the removal of the exemption needed to be reconciled with other legislative requirements, such as those under workplace relations legislation. It submitted that any reform should balance the interests of the individual with the need of the organisation to operate effectively.[115]

Other benefits of removing the exemption

40.60 The OPC noted that, in its 2007 survey on the Australian community's attitude towards privacy, 86% of the respondents considered that employees should have access

---

109 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; New Zealand Privacy Commissioner, *Submission PR 128,* 17 January 2007.

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

111 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

112 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

113 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

114 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

115 Australasian Compliance Institute, *Submission PR 419,* 7 December 2007.

to their personal information held by their employers.[116] It submitted that removing the employee records exemption would reflect community expectations.[117] In addition, the OPC stated that removing the exemption could have a number of other benefits, including:

- offering an appropriate balance between the interests of the parties, just as it offers such a balance between organisations and their customers
- providing a minimum set of standards for privacy protection of employee records, consistent with protection of an employee's rights as a private citizen
- providing certainty about rights and obligations for employers and employees
- eliminating regulatory difficulties in interpreting the exemption
- providing access to a conciliation-based complaints process through the Office of the Privacy Commissioner.[118]

40.61 The OVPC submitted that removing the exemption would promote a wider awareness and acceptance of privacy laws by private sector employees handling consumers' personal information. Further, it would result in better corporate decision-making and accountability, because privacy principles require improved information-handling practices. In addition, removing the exemption would standardise personal information-handling practices, which would be desirable in light of technologies such as email, DNA testing, radio frequency identification, and various workplace security and authentication measures using biometrics.[119]

40.62 Australia Post suggested that removing the exemption also could result in the streamlining and standardisation of work flows, and a reduction in costs relating to information technology, staff training and compliance.[120]

Arguments for retaining the exemption

40.63 In response to DP 72, stakeholders raised a number of arguments in support of retaining the employee records exemption. These arguments are discussed below.

Management and the employment relationship

40.64 Some stakeholders submitted that the exemption strikes an appropriate balance between the interests of employers and those of employees.[121] The AIG and AEEMA

116 See Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), 52.
117 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
118 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
119 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
120 Australia Post, *Submission PR 445*, 10 December 2007.
121 Confidential, *Submission PR 529*, 21 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

argued, for example, that this balance should take into account the employer's need to keep and utilise records for a wide range of legitimate business purposes.[122] When a person accepts employment with an organisation, it was suggested, he or she accepts that the employer will retain and use personal information for these purposes.[123]

40.65 Some stakeholders expressed concern that removing the employee records exemption would undermine the capacity of organisations to manage employees.[124] For example, Telstra submitted that removing the exemption, together with the introduction of the proposed statutory cause of action for a serious invasion of privacy,[125] would result in privacy claims that would either prevent an organisation from collecting employees' personal information, or require organisations to disclose otherwise confidential and sensitive information. Such privacy claims, it was argued, would undermine and frustrate significantly a business's capacity to deal with matters that would otherwise be regulated by the contract of employment.[126]

40.66 Another stakeholder submitted that removing the employee records exemption would restrict its routine management activities, such as the conduct of investigations, liaison with insurers and activities undertaken to comply with its statutory obligations under other legislation.[127] The ACCI stated that the employee records exemption provided employers with certainty, efficiency and flexibility in their human resources management practices. It argued that the removal of the exemption would undermine the ability of a business to manage its human capital effectively and would require changes in human resource management practices.[128]

40.67 Some stakeholders suggested that the special nature of the employment relationship, compared to other commercial relationships, justifies retaining the

---

122 Legitimate business purposes were said to include: the efficient operation of the business; compliance with legal obligations, such as those under OH&S laws; obtaining information for staff recruitment and selection processes; facilitating staff development; identifying poor performance, or inappropriate or unlawful behaviour, by an employee; defending legal claims brought by employees and former employees; and conducting due diligence when businesses are being outsourced or sold: Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494,* 19 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007.

123 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494,* 19 December 2007.

124 Confidential, *Submission PR 536,* 21 December 2007; Telstra Corporation Limited, *Submission PR 459,* 11 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007; Australian Business Industrial, *Submission PR 444,* 10 December 2007.

125 The statutory cause of action for invasion of privacy is discussed in Ch 74.

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

127 Confidential, *Submission PR 536,* 21 December 2007.

128 Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007. See also Australian Business Industrial, *Submission PR 444,* 10 December 2007.

employee records exemption.[129] They argued that, unlike most relationships regulated by the NPPs, the employment relationship is ongoing,[130] is often fiduciary,[131] and places a range of unique duties and obligations on the parties, such as the obligation of mutual trust and confidence.[132]

40.68 The ACCI argued that, if the employee records exemption were removed, any unintentional mistakes made by employers in the handling of their employees' personal information would diminish the relationship of trust and confidence between employers and employees.[133] Telstra submitted that removing the employee records exemption could affect adversely the sharing of personal information in the workplace in appropriate circumstances, such as the provision and administration of flexible work arrangements, team building exercises and personal development programs.[134]

Interaction with other legal obligations

40.69 Stakeholders noted that the employment relationship is subject to multiple laws relating to workplace relations, surveillance, whistleblowing and anti-discrimination.[135] Some employer groups submitted that employers handle employee records mostly for the purposes of complying with statutory requirements aimed at protecting the interests of employees.[136]

40.70 The handling of such records, it was argued, is an essential consequence of the employment relationship.[137] In particular, the collection, use and disclosure of health information about employees was said to be a necessary part of the employment

---

129 Confidential, *Submission PR 529*, 21 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

130 Confidential, *Submission PR 536*, 21 December 2007.

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

132 Confidential, *Submission PR 536*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. Case law characterises the employment relationship as a relationship of mutual trust and confidence: *Malik v Bank of Credit & Commerce International SA (in liq)* [1998] AC 20 ; *Blaikie v South Australian Superannuation Board* (1995) 65 SASR 85; *Brackenridge v Toyota Motor Corporation Australia Ltd* (1996) 142 ALR 99; *Burazin v Blacktown City Guardian Pty Ltd* (1996) 142 ALR 144; *Jager v Australian National Hotels Pty Ltd* (1998) 7 Tas R 437. Both the employer and the employee have a duty 'not to abuse or destroy the relationship of trust': R Owens and J Riley, *The Law of Work* (2007), 255.

133 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

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

135 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

136 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007.

137 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007.

contract.[138] Employers need to collect, use and disclose employees' health information, for example, in order to fulfil their legal obligations to protect the health and safety of their employees and the public.[139]

40.71 Australian Business Industrial expressed concern that removing the employee records exemption could prevent employers from requiring employees to present medical certificates for the approval of paid personal leave. The *Workplace Relations Act* authorises, but does not require, an employer to collect a medical certificate from an employee for the purposes of approving the taking of paid personal leave by the employee.[140] Requirements concerning the collection of sensitive information could, it was submitted, prevent the collection of sensitive health information contained in a medical certificate.[141]

40.72 The Recruitment and Consulting Services Association Australia and New Zealand submitted that, if the employee records exemption were removed, specific exceptions should be enacted to permit an employer or a recruitment company to collect, use or disclose an individual's personal health information without consent in certain circumstances—provided that the individual reasonably would expect the employer or recruitment company to handle such information for those purposes.[142]

40.73 Some employers contended that removing the employee records exemption could have an adverse impact on their ability to handle workers compensation claims and other associated employment-related litigation.[143] One stakeholder noted that it provided to its insurer personal information about its employees for the purpose of workers compensation claims on a regular basis. It argued that, if an employer were required to obtain the consent of the employee before disclosing such information, the insurance and rehabilitation approval process would be delayed significantly, to the detriment of the employee.[144]

Outsourcing arrangements

40.74 Optus noted that it is not uncommon for employers to outsource some of their employment-related activities to other companies. Examples of such outsourced

---

138 Australian Business Industrial, *Submission PR 444*, 10 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

139 Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007.

140 *Workplace Relations Act 1996* (Cth) s 254.

141 Australian Business Industrial, *Submission PR 444*, 10 December 2007.

142 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

143 Confidential, *Submission PR 536*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See also Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

144 Confidential, *Submission PR 536*, 21 December 2007.

activities included the recruitment of contractors and casual staff, the conduct of exit interviews and the provision of a salary package. Optus stated that there is uncertainty about whether the disclosure by employers of personal information about their employees to such companies would fall within the reasonable expectations of the employees. It suggested that removing the employee records exemption could prevent the exchange of information on a commercial-in-confidence basis in this context.[145]

Sale of businesses

40.75 The sale and purchase of a business may involve the collection and disclosure of personal information about different individuals, including employees, contractors, customers, trading partners and business associates.[146] Before the completion of a sale, the vendor may disclose such personal information to the prospective purchaser for the purposes of 'due diligence' investigations.[147]

40.76 Under existing law, the employee records exemption may apply to exempt the disclosure of employee records by a vendor organisation during the potential sale of its business. This would be the case where the disclosure relates directly to a current or former employment relationship between the vendor and the individual concerned.[148]

40.77 Some stakeholders considered that removing the employee records exemption would prevent an employer from disclosing personal information about employees to a potential purchaser of the employer's business, and interfere substantially with a potential purchaser's ability to conduct due diligence for the purposes of a business acquisition.[149]

40.78 Stakeholders submitted that prospective vendors of a business should be allowed to use and disclose employees' personal information without the consent of the employees.[150] Employee records that would be relevant in this context include records

---

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

146 See Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002), 1–2.

147 'Due diligence' is 'the process of acquiring objective and reliable information on a person or a company as required, especially before a commercial acquisition': *Macquarie Dictionary* (online ed, 2007). The collection, use and disclosure of employee records during due diligence may be protected by confidentiality agreements between vendors and prospective purchasers of the business: Optus, *Submission PR 532*, 21 December 2007.

148 *Privacy Act 1988* (Cth) s 7B(3).

149 Optus, *Submission PR 532*, 21 December 2007; Confidential, *Submission PR 529*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007.

150 Optus, *Submission PR 532*, 21 December 2007; Confidential, *Submission PR 529*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007.

concerning: time and wage records;[151] terms and conditions of employment,[152] including enterprise bargaining agreements, and applicable state and federal awards and agreements;[153] the level of leave entitlement;[154] details of trade unions of which employees are members;[155] records of claims made by employees;[156] potential issues related to OH&S or workers compensation;[157] and employees' conduct that may give rise to potential legal actions, such as unfair dismissal or anti-discrimination claims.[158]

40.79 In DP 72, the ALRC expressed the view that an exception or exemption for the use and disclosure of employee records in the context of due diligence is not warranted because the vendor organisation can either disclose aggregate information that does not identify individual employees, or obtain the consent of the individual employee where it is necessary to disclose the employee's personal information.[159]

40.80 In response, Telstra submitted that aggregated information about employees would be sufficient only for the early stages of a business transaction that involves the potential transfer of staff. It argued that, in order to complete the sale of the business, the vendor would have to disclose personal information about individual employees so that the potential purchaser may assess the quality or capability of the business and decide which employees to retain.[160]

40.81 The Motor Traders Association of NSW also submitted that prospective purchasers of a business and their lawyers, financial advisers and corporate advisers may need to review both aggregated and personal information about employees. It argued that, where the value of a business is linked directly to the expertise of its staff, more personal information about employees would need to be disclosed during the due diligence process than would otherwise be the case. Removal of the employee records exemption would have cost implications for the performance of due diligence inquiries.[161]

40.82 Some stakeholders expressed concern that it could be impractical, and in some cases, unlawful, for an employer to seek the consent of its employees to the disclosure of their personal information for the purposes of the potential sale of the employer's

---

151 Confidential, *Submission PR 529,* 21 December 2007; Motor Traders Association of NSW, *Submission PR 429,* 10 December 2007.
152 Confidential, *Submission PR 529,* 21 December 2007.
153 Motor Traders Association of NSW, *Submission PR 429,* 10 December 2007.
154 Confidential, *Submission PR 529,* 21 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
155 Motor Traders Association of NSW, *Submission PR 429,* 10 December 2007.
156 Ibid.
157 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
158 Ibid.
159 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [36.83].
160 Telstra Corporation Limited, *Submission PR 459,* 11 December 2007.
161 Motor Traders Association of NSW, *Submission PR 429,* 10 December 2007.

business.[162] For example, GE Money Australia contended that it often would be impossible for an employer to seek such consent because there could be legal obligations or considerations of commercial sensitivity that would prevent an employer from disclosing the fact of a potential sale of the business.[163] The ACCI argued that:

> The process of obtaining individual consent may not cause undue delay in a small business involving a few employees, but where large mergers and acquisitions of businesses occur, hundreds (and often thousands) of employees accept employment with the new employer. Delays and costs will undoubtedly ensue if each and every transferring employee is required to provide consent to disclose information contained in employment records.[164]

40.83 One stakeholder argued that if the employee records exemption were removed, there should be an exception to the 'Use and Disclosure' principle in the model UPPs to allow an organisation to disclose personal information to third parties for the purposes of due diligence as part of the sale of a business, or the transfer of employees as a result of the restructure of corporate entities.[165]

40.84 The OPC, in collaboration with the Law Council of Australia, has developed detailed guidance on the application of key NPPs to due diligence and completion for the sale and purchase of a business.[166] While the vendor's handling of employee records in the course of the sale generally are exempt from the operation of the *Privacy Act*, the OPC's guidance is relevant to a consideration of how personal information about employees should be handled after the removal of the exemption for two reasons:

- the vendor's handling of other personal information—such as the personal information of contractors, customers, trading partners and business associates—during the sale are not exempt from the operation of the *Privacy Act*; and

- the employee records exemption does not apply to the actions of the prospective purchaser in its handling of the vendor's employee records—unless and until it becomes the employer of the individual concerned.[167]

40.85 In the United Kingdom, the *Data Protection Act 1998* (UK)—which does not contain an exemption for employee records—also has been the subject of guidance

---

162 GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 529*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007. See also Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

163 GE Money Australia, *Submission PR 537*, 21 December 2007.

164 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

165 Confidential, *Submission PR 529*, 21 December 2007.

166 Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002).

167 See Ibid, 3.

issued by the Information Commissioner's Office (ICO) concerning mergers, acquisitions or business re-organisation.[168]

Regulatory burden and compliance costs

40.86 Stakeholders suggested that removing the employee records exemption would result in an additional regulatory burden and an increase in the costs of compliance for businesses.[169] The ABA, for example, noted the size and cost of tracking information collected about an employee from various sources within an organisation that is as large and complex as a bank. Further, such information may not be held centrally or in a readily retrievable form.[170]

40.87 The ACCI argued that, while education campaigns and funding would assist employers to understand regulatory changes, it would not reduce initial and ongoing compliance costs on businesses, such as legal advice, data storage, staff training and loss of productivity due to the need to deal with requests for access to personal information. The ACCI also submitted that any removal or modification of the exemption would involve a substantial increase in administrative resources, including the possibility that employers may have to appoint a dedicated privacy compliance officer.[171]

40.88 Another stakeholder stated that it regularly discloses information about its employees to a range of third parties, such as rehabilitation providers, employed medical practitioners and unions. It submitted that any requirement to obtain its employees' consent each time it sought to use and disclose information about its employees other than for the primary purpose of its collection would significantly increase the cost and resources required to manage its business effectively.[172]

40.89 Some stakeholders expressed concern that removing the employee records exemption, together with the requirements under the 'Cross-border Data Flows' principle, would result in an additional regulatory burden for those organisations that

---

168 United Kingdom Government Information Commissioner's Office, *The Employment Practices Code* (2005).

169 Confidential, *Submission PR 536*, 21 December 2007; Motor Trades Association of Australia, *Submission PR 470*, 14 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Australian Business Industrial, *Submission PR 444*, 10 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; IBM Australia, *Submission PR 405*, 7 December 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007 (endorsed by the National Australia Bank, *Submission PR 408*, 7 December 2007); Abacus–Australian Mutuals, *Submission PR 174*, 6 February 2007; Australian Retailers Association, *Submission PR 131*, 18 January 2007.

170 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

171 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

172 Confidential, *Submission PR 536*, 21 December 2007.

transfer and hold internal human resources data overseas.[173] GE Money Australia noted that organisations that operate in a number of countries commonly maintain information about all their employees in a single system that may be hosted in one country. GE Money expressed concern that removing the employee records exemption, coupled with the requirements under the 'Cross-border Data Flows' principle, could impede the collection and recording of employees' personal information in an accurate and efficient way.[174]

40.90 On the other hand, some stakeholders submitted that the additional costs of compliance resulting from removing the employee records exemption could be mitigated by certain factors.[175] The OPC submitted:

> The Office understands that many large businesses already apply the privacy principles to their handling of employee records. For those businesses any removal of the exemption may not create an added compliance cost. Conversely for those businesses that do not currently apply the NPPs to their employee records there would be costs to implement and maintain a compliance regime.[176]

40.91 Similarly, AAMI submitted that, in practice, larger businesses already had procedures in place to ensure that their employees' personal information would be treated in the same way as other personal information that was covered by the *Privacy Act*.[177]

40.92 The Office of the Information Commissioner (Northern Territory) submitted that 'in the absence of clear evidence to the contrary … the extent of the additional costs to business of removal of the employee records exemption should not be assumed or overstated'. The Office stated that the increase in resources required to include private sector employee records within the existing scheme may be 'marginal', on the basis that:

- since most businesses that are currently subject to the *Privacy Act* are required to handle personal information (other than employee records) in accordance with the Act, they already would have in place mechanisms for developing policies to implement the NPPs and procedures for dealing with complaints about breaches of the NPPs;

- there is growing expertise in dealing with privacy issues within the workforce because of the extensive coverage of privacy legislation; and

---

173 GE Money Australia, *Submission PR 537*, 21 December 2007; Australian Information Industry Association, *Submission PR 410*, 7 December 2007; IBM Australia, *Submission PR 405*, 7 December 2007.

174 GE Money Australia, *Submission PR 537*, 21 December 2007.

175 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; AAMI, *Submission PR 147*, 29 January 2007.

176 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

177 AAMI, *Submission PR 147*, 29 January 2007.

- removing the employee records exemption would simplify the structure of the *Privacy Act*, reducing the current costs of interpreting and applying the exemption.[178]

Application of the UPPs to existing employees

40.93 Some stakeholders suggested that, if the employee records exemption were removed, there would be administrative difficulties in obtaining the consent of existing employees to the handling of personal information by their employers.[179] It was suggested that the *Privacy Act* should not apply to existing employees because consent to the use and disclosure of their records could amount to a variation of the employment contract. Further,

> If an employee refused to consent to his or her information being used or disclosed, for example, to monitor the employee's conduct or performance, this could hinder [its] disciplinary procedures and compromise the safety of its employees.[180]

Privacy codes or non-binding guidelines

40.94 Some stakeholders supported promoting privacy protection of employee records through the use of non-binding best practice guidelines or privacy codes, rather than by removing the employee records exemption.[181] DEWR stated that guidelines were likely to be met with greater support from employer groups.[182] Another stakeholder submitted that guidelines would assist in ensuring fairness in workplace practices concerning the collection and utilisation of employees' personal information, while privacy codes developed by organisations would be more flexible than legislation in that they could be tailored to meet the needs of a particular organisation.[183] In addition to guidelines and privacy codes, the ACCI also supported 'the formulation of educational initiatives to better inform employers and employees of their rights and obligations regarding employee records'.[184]

---

178 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

179 Confidential, *Submission PR 536*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007. Employee records include not only formal records held in a centralised and secure area, but also day-to-day operational records kept by an employee's immediate manager, such as conversations about the employee's performance and staff training records: Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

180 Confidential, *Submission PR 536*, 21 December 2007.

181 Confidential, *Submission PR 529*, 21 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.

182 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.

183 Confidential, *Submission PR 529*, 21 December 2007.

184 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.

ALRC's view

40.95 Employee records can contain a significant amount of personal information about employees, including sensitive information such as health and genetic information. There is a real potential for individuals to be harmed if employees' personal information is used or disclosed inappropriately. The lack of adequate privacy protection for employee records in the private sector is of particular concern because employees may be under economic pressure to provide personal information to their employers.

40.96 According to the Australian Bureau of Statistics (ABS), 84% of Australians are employed in the private sector.[185] The lack of privacy protection for the majority of Australian employees is unjustifiable and represents a significant gap in privacy regulation. There is no sound policy reason why privacy protection for employee records only is available to public sector employees and not private sector employees; or for treating employees' personal information differently from other personal information.

40.97 At the time the private sector provisions of the *Privacy Act* were introduced, the Australian Government acknowledged that employee records deserve privacy protection, but considered that the issue would be more appropriately dealt with in workplace relations legislation. More than seven years after the enactment of the private sector provisions, however, workplace relations legislation still does not provide sufficient privacy protection for employee records.

40.98 Privacy legislation in comparable overseas jurisdictions, such as the United Kingdom and New Zealand, does not contain an exemption that applies to employee records. Removing the employee records exemption would bring Australian privacy law closer to that in comparable overseas jurisdictions, and may facilitate recognition of the adequacy of Australian privacy law by the EU.

40.99 As discussed above, stakeholders raised a number of objections to the removal of the employee records exemption. These objections are considered below.

Management and the employment relationship

40.100 The application of the model UPPs to employee records need not interfere with the business or management interests of employers or with employment relationships. In general terms, the model UPPs require that the employer:

- obtain the consent of its employees in appropriate circumstances—for example, where the employer wishes to collect sensitive information about an employee,

185 As at May 2007, there were 10,439,700 employed persons who were aged 15 and over, of which 1,662,300 were federal, state and local government employees: Australian Bureau of Statistics, *Australian Labour Market Statistics*, 6105.0 (2008), 13, 35.

or to use or disclose information for a purpose that is unrelated to the primary purpose of collection; and

- take reasonable steps to ensure that its employees are aware of the matters listed in the 'Notification' principle, such as the purpose for which personal information is collected, and employees' rights of access to, and correction of, that information.

40.101 The removal of the employee records exemption will not result in organisations being required to disclose otherwise confidential and sensitive information. There are a number of exceptions to the 'Access and Correction' principle in the model UPPs that would allow an employer to deny a request for access by an employee to his or her personal information in certain circumstances, including where, for example, providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.[186]

40.102 The removal of the employee records exemption would not undermine the ability of businesses to manage their human resources effectively. On the contrary, good information-handling practices would assist in ensuring that organisations would be making sound business decisions based on accurate and up-to-date information that is held securely within the organisation.

40.103 Aspects of the employment relationship reinforce, rather than negate, the need to ensure that the privacy of employee records is protected adequately. Mutual trust and confidence, on which the employment relationship is said to be based, is enhanced by the open and fair handling of employee records in accordance with the privacy principles. Further, the fact that an employment relationship is ongoing, and employee records may be used for a range of business purposes over time, serves to highlight, rather than diminish, the need for privacy protection.

Interaction with other legal obligations

40.104 The removal of the employee records exemption from the *Privacy Act* would not interfere with employers' existing obligations under other laws—such as laws concerning workplace relations, OH&S, workers compensation, anti-discrimination and unfair dismissal.

40.105 The model UPPs contain specific exceptions to the 'Collection', 'Use and Disclosure' and 'Access and Correction' principles that allow organisations to collect,

186 The treatment of 'evaluative material' under the *Privacy Act* is discussed in more detail below.

use, disclose and deny access to personal information (including sensitive information) about an individual where this is 'required or authorised by or under law'. Accordingly, employers would be able to collect, use, disclose or deny access to personal information where this is necessary to enable them to meet their legal obligations under other laws.

40.106 In particular, the 'Collection' principle in the model UPPs allows the collection of sensitive information where the collection is 'required or authorised by or under law' instead of 'required by law', as is presently the case under NPP 10.1(b).[187] This reform addresses the concerns that employers may be prevented from collecting medical certificates for the approval of paid personal leave under the *Workplace Relations Act*.[188]

Outsourcing arrangements

40.107 The fact that the employee records exemption currently allows an organisation to disclose personal information about employees to an unrelated company suggests that the exemption should be removed. There is no good policy reason why organisations should be permitted to disclose employees' personal information other than in accordance with the 'Use and Disclosure' principle in the model UPPs.

40.108 The 'Use and Disclosure' principle would allow an organisation to disclose personal information about an employee for a secondary purpose where the disclosure: is related to the primary purpose of collection of that information (or, in the case of sensitive information, directly related to the primary purpose of collection); and is within the reasonable expectations of the individual.

40.109 Where outsourced activities are employment related, the disclosure of an employee's personal information to a contractor may be related to the primary purpose of collection and within the reasonable expectations of the employee. Where this is not the case, the employer should ensure that the individual consents to the disclosure.

Sale of businesses

40.110 The removal of the employee records exemption would not hamper the ability of organisations to buy and sell businesses. Guidance issued by the OPC and, in the United Kingdom by the ICO, suggests a number of ways in which vendors and prospective purchasers can handle personal information during the sale and purchase of a business, while ensuring compliance with privacy principles.

40.111 First, the vendor should provide aggregate, non-identifiable information about employees to the prospective purchaser whenever possible. Such information would not fall within the definition of 'personal information' in the *Privacy Act* and therefore

187 See Ch 22, Rec 22–2.
188 See *Workplace Relations Act 1996* (Cth) s 254.

would not be covered by the Act.[189] The prospective purchaser may conduct due diligence inquiries by inspecting records and making a note of the fact that the records have been inspected (without recording the details of the personal information inspected), which would not constitute 'collection' of the personal information for the purposes of the *Privacy Act*. Secondly, where disclosure of personal information about employees to the prospective purchaser is required, the vendor is not necessarily obliged to obtain the consent of the employee. Arguably, the disclosure of employee records to a prospective purchaser of a business is directly related to the primary purpose of collection, and within the individual's reasonable expectation.[190] In some cases, the vendor also may have a legal obligation to avoid alerting employees to the possibility of a transmission of business, for example, where to do so is prevented by a prohibition against 'insider trading'.[191]

40.112 Further, where the prospective purchaser collects personal information about employees from the vendor, the prospective purchaser is not necessarily required to take steps to advise the employee about the matters listed in the 'Notification' principle. Due diligence processes may need to be conducted confidentially in order to protect the interests of the organisations involved. The OPC has stated that:

> the [Privacy] Commissioner takes the view that, even if personal information is recorded by a prospective purchaser, it would generally be reasonable at this time for the prospective purchaser organisation to take no steps under NPP 1.5 to advise the individual about whom personal information is collected of the NPP 1.3 matters. However, taking no steps would only be reasonable where the prospective purchaser organisation decides not to proceed with the purchase of the business, and returns or destroys all records of personal information to the vendor organisation.[192]

Regulatory burden and compliance costs

40.113 The removal of the employee records exemption would result in some additional compliance costs for some employers. The ALRC is not persuaded, however, that avoiding these costs provides a sufficient policy basis to support the retention of the employee records exemption. In any case, the costs to businesses resulting from removal of the exemption should not be overestimated.

---

189 Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002), 3–4. See also United Kingdom Government Information Commissioner's Office, *The Employment Practices Code* (2005), [2.12.1].

190 See, by analogy, the OPC's guidance relating to the disclosure of other personal information to the prospective purchaser of a business: Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002), 2–3. See also United Kingdom Government Information Commissioner's Office, *The Employment Practices Code—Supplementary Guidance* (2005), [2.12.3].

191 See United Kingdom Government Information Commissioner's Office, *The Employment Practices Code* (2005), [2.12.3].

192 Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002), 4.

40.114 The organisations which will carry the greatest burden—that is, large businesses—already are required to comply with the *Privacy Act* in relation to other personal information and therefore, already have in place mechanisms and procedures for the handling of personal information. Additionally, many businesses already handle employee records in the same way they handle other personal information.

40.115 Further, more than half of existing Australian businesses are not employers. According to the ABS's most recent figures, as at June 2007, there were 2,011,770 actively trading businesses in Australia, of which 1,171,832 (58%) were non-employing.[193] There will be more than one million actively trading businesses, therefore, that will not be affected by the removal of the employee records exemption.

40.116 Elsewhere in this Report, the ALRC makes a number of recommendations aimed at reducing the complexity of the existing privacy regime. These include recommendations that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity, and that the privacy principles be streamlined.[194] The simplification of the legislation should go some way towards reducing the costs of compliance for employers.

40.117 The requirements under the 'Cross-border Data Flows' principle would not result in any significant additional burden for those organisations that transfer and hold internal human resources data overseas. The principle does not prevent personal information from being transferred or require any additional steps to ensure compliance with the *Privacy Act*. It merely requires that an organisation remain accountable for any transfer of personal information overseas, except in defined circumstances.[195]

Application of the UPPs to existing employees

40.118 As discussed above, removing the employee records exemption would not result in employers being required to obtain the consent of existing employees for the use and disclosure of their personal information in every case. The employer only would have to obtain the consent of its employees if: it wishes to use or disclose the employees' personal information for a secondary purpose that is not related—or in the case of sensitive information, not *directly* related—to the primary purpose of collection; and the use or disclosure is not within the reasonable expectations of the employee. Since existing employee records generally would have been collected for the primary purpose of the employment relationship, in most cases, there would not be a need to obtain the consent of existing employees for the use and disclosure of their personal information.

193 Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), 18.
194 See Recs 5–2, 18–2.
195 See Ch 31.

40.119 Where an employer wishes to use or disclose an employee's personal information for a secondary purpose that is unrelated to the employment relationship, such use and disclosure would not form part of the employment relationship and therefore the requirement to obtain the employee's consent would not amount to a variation of the employment contract.

Privacy codes or non-binding guidelines

40.120 The use of privacy codes or non-binding guidelines is not a substitute for legislative protection and would not be a sufficient response to the significant concerns raised about the lack of privacy protection for employee records. Such initiatives would not resolve the issue of inconsistent regulation of employee records between the public and private sectors. Again, there is no good policy basis to justify treating employee records differently from other personal information.

Conclusion

40.121 For these reasons, the ALRC recommends that the employee records exemption be removed. Removing the exemption would ensure that the privacy of employee records held by organisations is protected under the *Privacy Act*, and that employees' sensitive information, such as health and genetic information, is given a higher level of protection under the Act. This protection should be in addition to that provided by other laws, such as the relevant provisions in the *Workplace Relations Regulations*.

40.122 Having regard to the various concerns raised by employers and employer groups, the OPC should develop and publish specific guidance on the application of the UPPs to employee records to assist employers in fulfilling their obligations under the *Privacy Act*. This guidance should address, in particular, concerns about when it is and is not appropriate to disclose to an employee concerns or complaints by third parties about the employee. These concerns are discussed in detail below, in relation to the handling of 'evaluative material' about employees.

Recommendation 40–1 The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.

Recommendation 40–2 The Office of the Privacy Commissioner should develop and publish guidance on the application of the model Unified Privacy Principles to employee records, including when it is and is not appropriate to disclose to an employee concerns or complaints by third parties about the employee.

Evaluative material

40.123 The 2000 House of Representatives Committee inquiry acknowledged that there is a difference between an employee's health, family and financial information—which should not be provided to anyone else without the consent of the employee—and information concerning disciplinary matters or career progression of the employee.[196] The inquiry went on to recommend a significant narrowing of the scope of the employee records exemption in the *Privacy Act* to apply only to 'exempt employee records', which would consist of records relating to: the engagement, training, disciplining or resignation of the employee; termination of employment; and the employee's performance or conduct.[197]

40.124 The inquiry recommended that the other matters listed in the proposed definition of 'employee record' be subject to the NPPs. It also noted that employee records can contain personal and sensitive information regardless of the size of the employer and therefore was of the view that its recommendations also should apply to small business employers.[198] The inquiry's recommendations were not intended to override the provisions in the workplace relations legislation.[199] These recommendations were rejected by the Australian Government.[200]

Employment references

40.125 In DP 72, the ALRC acknowledged the concern raised by some stakeholders that the removal of the employee records exemption could affect the ability of prospective employers to engage in full and frank communication with a job applicant's previous employers.[201] A major concern, in this context, is that employers may not provide references, or accurate and honest references, if employees are able to obtain access to them.

40.126 At common law, an employer (or a former employer) does not have an obligation to provide a reference for an employee.[202] Where the employer or former employer does provide a reference, however, the employer will be subject to the laws of defamation and deceit. The employer also may be under a duty to take reasonable care to ensure that the factual content of the reference is accurate and the opinion

---

196 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.36].

197 Ibid, recs 5–7.

198 Ibid, [3.40].

199 Ibid, [3.39].

200 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

201 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; UNITED Medical Protection, *Submission PR 118*, 15 January 2007; M Hunter, *Submission PR 16*, 1 June 2006.

202 *Carrol v Bird* (1800) 170 ER 588.

expressed is reasonably held.[203] It has been argued that, when faced with potential legal liability, employers may cease to provide references or use a disclaimer. In addition, where an employee is able to gain access to the reference, there could be social pressures that prevent complete honesty from referees.[204]

40.127 In contrast, it may be argued that it is impossible to predict how imposing a duty of care on employers would, in practice, affect the flow of such information. Many employers already take considerable care in preparing references and, therefore, the imposition of a legal obligation on employers to prepare references with care might not deter them from providing a reference. In addition, such a legal obligation might improve the quality of the information. As a result, reducing the quantity of references might not harm the public interest in the provision of full and frank references.[205]

Discussion Paper proposal

40.128 In order to address concerns about the handling of references and similar personal information, in DP 72, the ALRC considered three options for reform.

40.129 One option would be to exclude personal references given by referees from the operation of the *Privacy Act*. The Canadian *Privacy Act 1985* defines 'personal information' to exclude 'the personal opinions or views of the individual … about another individual'.[206] Similarly, in New South Wales, s 4(3)(j) of the *Privacy and Personal Information Protection Act 1998* (NSW) provides that the definition of 'personal information' excludes 'information or an opinion about an individual's suitability for appointment or employment as a public sector official'.

40.130 Another option would be to amend the *Privacy Act* to allow the recipient of a reference to deny a request for access to a reference that is given to it in confidence. Under s 29 of the *Privacy Act 1993* (NZ), an agency may deny a request for access to evaluative material, disclosure of which would breach a promise of confidence to the supplier of the information. 'Evaluative material' is defined to mean:

> evaluative or opinion material compiled solely—
>
> (a) For the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates—
>
> (i) For employment or for appointment to office; or
>
> (ii) For promotion in employment or office or for continuance in employment or office; or

---

203 *Spring v Guardian Assurance Plc* [1995] 2 AC 296; applied in *Wade v Victoria* [1999] 1 VR 121.

204 J Catanzariti, 'Are the Days of the Employee Reference Numbered?' (1996) 34(8) *Law Society Journal* 31, 31.

205 T Allen, 'Liability for References: The House of Lords and Spring v Guardian Assurance' (1995) 58 *Modern Law Review* 553, 556–557.

206 *Privacy Act* RS 1985, c P-21 (Canada) s 3.

> (iii) For removal from employment or office; or
>
> (iv) For the awarding of contracts, awards, scholarships, honours, or other benefits; or
>
> (b) For the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or
>
> (c) For the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.[207]

40.131 A third option would be to allow a potential employer to deny access to a personal reference given by a referee until after the job applicant has been informed of the result of the recruitment process. In Hong Kong, s 56 of the *Personal Data (Privacy) Ordinance* provides that, unless the referee consents, a data user does not have to provide a job applicant with access to, or a copy of, a personal reference given by the referee until after the job applicant has been informed in writing that he or she has been accepted or rejected to fill that position or office.[208]

40.132 The ALRC expressed the preliminary view that there was sufficient ground for an exception to the 'Access and Correction' principle, provided that a personal reference was given in confidence to a potential employer. The ALRC noted that this was in line with the common law obligation of confidence. At common law, an action for breach of confidence may arise where:

- the information has the 'necessary quality of confidence'—that is, it must be non-trivial, and, to some extent, secret or inaccessible;
- the information was communicated or obtained in such circumstances as to give rise to an obligation of confidence; and
- there is actual or threatened unauthorised use of the information.[209]

40.133 The ALRC observed that such an exception also would be in line with the existing law that applies to employees of Australian Government agencies. Although employment records of an Australian Government agency employee are covered by the *Privacy Act*, an employee is not entitled to access personal references about him or her held by an agency if their disclosure would found an action for breach of confidence.[210]

---

207 *Privacy Act 1993* (NZ) s 29(3).

208 *Personal Data (Privacy) Ordinance* (Hong Kong) s 56.

209 *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 56 ALR 193, 208.

210 Under IPP 6, a public sector agency may refuse a request by an individual for access to personal information that the agency holds to the extent that the agency is required or authorised to refuse access under an applicable Commonwealth law that provides for access by persons to documents: *Privacy Act 1988* (Cth) s 14 IPP 6. Under the *Freedom of Information Act 1982* (Cth), an agency may refuse to grant access to the documents if their disclosure under the Act would found an action by a person for breach of confidence: *Freedom of Information Act 1982* (Cth) ss 11, 45.

40.134 Accordingly, the ALRC proposed that the *Privacy Act* should provide for an exception to the proposed 'Access and Correction' principle in the model UPPs that would allow an agency or organisation to deny a request for access to 'evaluative material' that was given in confidence to an agency or organisation.[211] The proposed exception was based on the approach taken in the New Zealand *Privacy Act* rather than the other two options considered, because exceptions to the UPPs should be as narrowly drawn as possible. In addition, since the common law obligation of confidence endures for the duration of the confidential relationship, the ALRC did not consider that the exception should apply only until the end of the recruitment process.

40.135 The ALRC also stated that the same exception that would apply to confidential personal references also should apply to evaluative material compiled for the sole purpose of determining the awarding, continuation, modification or cancellation of contracts, awards, scholarships, honours or other benefits. This was because, in determining whether an individual should be awarded a contract, award or other similar benefits, the referee should be able to provide an honest evaluation about the individual's merits without fear of that evaluation being made available to the individual concerned. The ALRC therefore proposed that, in the context of the proposal, 'evaluative material' should be defined to mean evaluative or opinion material compiled solely for the purpose of determining the suitability, eligibility, or qualifications of the individual concerned for employment, appointment or the award of a contract, scholarship, honour, or other benefit.[212]

211 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 36–2.
212 Ibid, Proposal 36–2.

Submissions and consultations

Confidential employment references

40.136 Some stakeholders expressed support for the ALRC's proposal.[213] The OVPC stated that the proposal seemed to be 'fairly carefully worded', which was important to avoid overly broad interpretations.[214] Privacy NSW expressed 'cautious support' for the proposal and also noted that judicial interpretation of the New South Wales provision has caused difficulty for many employees seeking access to employment-related personal information.[215]

40.137 National Legal Aid expressed reservations about the proposal because the common law on liability for negligent references is still undeveloped. It stated that, given this state of development,

> There is scope for a more robust debate on whether those who provide references should be able to rely on confidentiality where information is malicious or intended to prevent an employee from obtaining employment elsewhere.[216]

40.138 Some stakeholders objected to the ALRC's proposed exception to the 'Access and Correction' principle concerning confidential evaluative materials.[217] Stakeholders submitted that modern human resources practices could and should accommodate the openness of referee reports.[218] PIAC, for example, stated that there were good reasons why current employees should be able to access evaluative records. Unfair referee

---

213 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; ANZ, *Submission PR 467*, 13 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007. Some stakeholders indicated that their support for the removal of the employee records exemption was contingent upon the implementation of the proposal that there be an exception relating to confidential evaluative material: 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.

214 The OVPC stated that the New South Wales provision has been interpreted so broadly that it effectively amounted to an employee records exemption: Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007, referring to *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(j); *Y v Director General, Department of Education & Training* [2001] NSWADT 149, [33], [36].

215 Privacy NSW, *Submission PR 468*, 14 December 2007, referring to *PN v Department of Education & Training* [2006] NSWADT 122 (upheld in *Department of Education & Training v PN (GD)* [2006] NSWADTAP 66).

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

217 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; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

218 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

reports can be an obstacle to continued employment;[219] and evaluative records can provide evidence of discrimination against employees on the basis of such characteristics as age, race, sex, disability and family responsibilities.[220]

40.139 Several stakeholders noted that the proposed UPPs already contained general exceptions that would address employers' concerns about the confidentiality of evaluative materials.[221] For example, the OPC submitted that there was no compelling policy reason to create a specific exception under the 'Access and Correction' principle because an exception capable of covering breach of confidence—that is, where 'providing access would be unlawful'—would continue to be incorporated in the principle.[222] The OPC also argued that there was no sound policy reason for treating evaluative material about employees or potential employees differently from other personal information under the *Privacy Act* and expressed concern about the consequent 'complexity and unnecessary compliance costs'.[223]

40.140 Other stakeholders noted that the proposed 'Access and Correction' principle provides for an exception where 'providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations'. They submitted that this exception should be sufficient to address any concerns employers might have about having to grant employees access to evaluative material.[224]

40.141 Some employers and employer groups objected to the ALRC's proposal for other reasons.[225] Suncorp-Metway Ltd maintained that the removal of the employee records exemption could prevent or discourage referees from giving a full and frank reference. It submitted this issue was of particular concern to the financial services industry because of its need to employ people of good character to handle financial and other personal information appropriately.[226]

---

219 See also Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

220 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

221 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.

222 NPP 6.1(g). The OPC has issued guidelines stating that this exception would cover circumstances where providing access would be a breach of confidence: Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001), 4.

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

224 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

225 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007.

226 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

40.142 The ACCI and the Retail Motor Industry suggested that the proposed exception concerning evaluative material could give rise to uncertainty.[227] In particular, the ACCI noted differing judicial views on breach of confidence and submitted that the right to deny access to evaluative material should not be based on the potential for such an action.[228]

40.143 Some stakeholders submitted that the scope of the proposed exception concerning evaluative materials was too limited.[229] GE Money Australia stated that the extent to which the exchange of evaluative material between employers would be permissible under the UPPs was unclear.[230] Another stakeholder submitted that the ALRC's proposal would result in job applicants seeking to exercise their right of access to evaluative materials with the supplier of those materials rather than the potential employer. It also submitted that there should be

> guidance to clarify when it would not be reasonable and practicable to collect information from the individual concerned, particularly where the information is required to validate or falsify information provided by a candidate in connection with an application to work, or to fill in gaps in a candidate's work history.[231]

Confidential complaints and investigation of misconduct

40.144 Some stakeholders expressed specific concern about the application of the *Privacy Act* to confidential complaints about an employee.[232] It was argued that, where the confidential complaint was made by one employee against another, requiring an employer to grant access to information about a complaint could compromise workplace relations,[233] and dissuade employees from raising concerns with their supervisors about other employees in appropriate circumstances.[234]

40.145 National Australia Bank stated that granting employees access to personal information contained in a confidential complaint made by their colleagues would be contrary to the duty of confidentiality owed by employers to their employees. It submitted that employees could be deterred from complaining, or would pursue

---

227 Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007; Retail Motor Industry, *Submission PR 407,* 7 December 2007.

228 Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007.

229 GE Money Australia, *Submission PR 537,* 21 December 2007; Law Council of Australia, *Submission PR 527,* 21 December 2007; Telstra Corporation Limited, *Submission PR 459,* 11 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007.

230 GE Money Australia, *Submission PR 537,* 21 December 2007.

231 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353,* 30 November 2007.

232 Confidential, *Submission PR 536,* 21 December 2007; Avant Mutual Group Ltd, *Submission PR 421,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

233 Confidential, *Submission PR 536,* 21 December 2007; Avant Mutual Group Ltd, *Submission PR 421,* 7 December 2007.

234 Confidential, *Submission PR 536,* 21 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

complaints through external avenues, which would not be conducive to a positive workplace environment.[235]

40.146 The National Catholic Education Commission and Independent Schools Council of Australia raised similar concerns in the context of confidential complaints about employees received from parents, students and staff. The Council noted that complaints about an employee were sometimes not disclosed to the employee so as not to harm the relationship between the employee and the complainant parent or the pupil. At other times, information would be passed on in a de-identified form. The Council suggested that there should be an additional exception to the 'Access and Correction' principle that allows an agency or organisation to deny access to confidential material compiled solely for the purposes of

> evaluating complaints or concerns about an employee where it is reasonably considered that giving access to the material may result in material of a similar nature not being provided in the future or unreasonably affect ongoing relationships.[236]

40.147 Several stakeholders submitted that the removal of the employee records exemption would have an adverse effect on the investigation of suspected employee misconduct, such as misappropriation, fraud, sabotage, bullying and harassment.[237] Telstra, for example, submitted that employees should not be granted access to statements, reports and evidence relating to the investigation of misconduct because this would prejudice the investigation, or would discourage victims, witnesses and whistleblowers from coming forward.[238] Telstra stated that evidence gathered against the employee during the investigation only should be available if proceedings were subsequently taken against the employee.[239]

Other evaluative materials

40.148 Some stakeholders suggested that, if the employee records exemption were to be reformed, provision should be made to exclude certain records from the requirements of the UPPs. These records included those concerning: the engagement,

---

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

236 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462,* 12 December 2007.

237 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; Confidential, *Submission PR 536,* 21 December 2007; Optus, *Submission PR 532,* 21 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 452,* 7 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

238 Telstra also argued that the removal of the employee records exemption could hinder the effectiveness of fitness for duty assessments and investigation of out-of-hours conduct for return-to-work programs under a workers compensation scheme: Telstra Corporation Limited, *Submission PR 459,* 11 December 2007.

239 Ibid.

training, disciplining, resignation or termination of an employee; and the performance or conduct of the employee.[240]

40.149 Another stakeholder noted that third parties—such as referees, managers, clients, complainants and work colleagues—often disclose personal information about an employee for these purposes. It was argued that, if the employee records exemption were removed, third parties and employers who disclose or grant access to personal information about an employee should be protected from legal action, such as defamation and workers compensation claims—especially in circumstances where they were required by the *Privacy Act* to grant access.[241]

40.150 Other stakeholders suggested that the proposed exception concerning evaluative materials should be extended to apply to:

- personal information relating to the ongoing evaluation and assessment of employees by employers;[242]
- evaluative materials concerning job applicants,[243] including information required for pre-employment screening;[244]
- the handling of health information about a job applicant without the applicant's consent for the purposes of assessing his or her suitability to perform particular types of work;[245] and
- all personal information included within the definition of 'employee record' in the *Privacy Act*.[246]

ALRC's view

40.151 As a general proposition, individuals should have a right to access all personal information about them, including evaluative materials in the employment context. The open and fair handling of employees' personal information, in accordance with the UPPs, should be required in all circumstances—including in potentially contentious

240 Law Council of Australia, *Submission PR 527*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007. The Law Council of Australia suggested that, alternatively, this class of records should be regulated by the UPPs generally, but should not be subject to the 'Access and Correction' principle: Law Council of Australia, *Submission PR 527*, 21 December 2007.

241 Confidential, *Submission PR 529*, 21 December 2007.

242 Law Council of Australia, *Submission PR 527*, 21 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

243 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

244 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007.

245 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

246 Australian Chamber of Commerce and Industry, *Submission PR 452*, 7 December 2007. See also Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

situations such as evaluation of performance, disciplinary action, resignation and termination of contract.

40.152 One concern raised by stakeholders is that the *Privacy Act* may require an employer to provide an employee with access to possibly unfavourable evaluative materials or opinions about the employee. In the ALRC's view, granting employees access to their personal information, including unfavourable evaluations, is part of the open and fair handling of that information.

40.153 There are a number of competing considerations, however, that may justify the denial of such access. These considerations include the interest in: maintaining confidentiality; protecting the privacy of third parties; ensuring organisations comply with other legal obligations that may require them to deny access; ensuring that access would not prejudice the investigation of possible unlawful activity; and allowing organisations to deny access to information connected with commercially sensitive decision-making.

40.154 The 'Access and Correction' principle in the model UPPs strikes an appropriate balance between providing employees with access and allowing employers to deny access in appropriate circumstances. There is no compelling reason to create additional exceptions or exemptions in the *Privacy Act* that apply specifically to evaluative materials.

40.155 The UPPs contain general exceptions that address employers' concern about the confidentiality of evaluative materials, such as employment references. In particular, the 'Access and Correction' principle in the model UPPs contains specific exceptions that would allow an organisation to deny access to a request for personal information in certain circumstances, including where: providing access would be unlawful; or denying access is required or authorised by law. Both of these exceptions would permit the employer to deny access if providing access would be a breach of confidence.[247] In addition, individuals generally would not be able to access confidential evaluative materials with the supplier of those materials, who would be exempt from the operation of the Act, if acting in his or her personal or non-business capacity.[248]

---

247 The references still would be accessible by the process of discovery in legal proceedings. In the case of employers that are agencies, such materials would be subject to the provisions of the *Freedom of Information Act 1982* (Cth).

248 *Privacy Act 1988* (Cth) ss 7B(1), 16E. The ALRC has expressed the view that the *Privacy Act* should retain an exemption for personal and non-business use of personal information: see Ch 43.

40.156 There also are concerns about the handling of personal information in the context of confidential complaints about employees. Again, in appropriate circumstances, qualifications and exceptions to the model UPPs lift the obligations to notify individuals about the collection of personal information and to provide access to it.

40.157 Under the 'Notification' principle, an organisation only is required to 'take such steps, if any, as are reasonable in the circumstances' to ensure that an individual is aware of the matters listed in the principle, such as the fact and circumstances of collection. An employer would not be required to notify an employee that it has received a complaint if it would not be reasonable to do so in the circumstances. Where the complaint is made in confidence to the employer, it would not be reasonable to require an employer to notify the employee who is the subject of the complaint if, for example, the complaint is not substantive enough to warrant investigation. Similarly, it would not be reasonable to require an employer to notify the employee of an investigation into suspected misconduct by the employee, if to do so would prejudice the investigation of the matter.

40.158 The 'Access and Correction' principle also contains specific exceptions that would allow an organisation to deny access to a request for personal information in certain circumstances, including where an employer is under an obligation of confidence to a complainant not to disclose the complaint about an employee to the employee. The employer also may deny a request for access by the employee to the confidential complaint on the basis that: providing access would be unlawful; denying access is required or authorised by law; or providing access would have an unreasonable impact on the privacy of the complainant.

40.159 Where an employer is conducting an investigation into suspected misconduct by an employee, the 'Use and Disclosure' principle in the model UPPs permits the use or disclosure of personal information by the employer about an employee if: it has reason to suspect that the employee is or may be engaged in unlawful activity (such as fraud or harassment); and the use or disclosure is a necessary part of its investigation or reporting its concerns to relevant persons or authorities. In addition, the employer may refuse to provide the employee with access to materials collected during the investigation if providing access would be likely to prejudice an investigation of possible unlawful activity. If legal proceedings against the employee are anticipated, the employer also may deny access on the basis that the information relates to anticipated legal proceedings between the organisation and the employee, and the information would not be accessible by the process of discovery in those proceedings.

40.160 While the UPPs are flexible enough to accommodate the handling of complaints about, and investigations into suspected misconduct by, employees, submissions by some stakeholders indicated that there might be some misconceptions as to how the UPPs would apply in these circumstances. Guidance issued by the OPC should address how the UPPs would apply to the handling of complaints about employees and the investigation of suspected employee misconduct.

40.161 Finally, the ALRC does not consider that there should be specific exceptions that permit an employer or a recruitment company to collect, use or disclose personal health information about a job applicant without the applicant's consent for the purposes of assessing his or her suitability to perform particular types of work.

40.162 Sensitive information, such as health information, should be collected with the consent of the individual—unless the collection is required or authorised by or under law, or falls within any other exceptions under the 'Collection' principle. Where health information is necessary for the assessment of the suitability of a job applicant to perform particular types of work and the applicant does not consent to the collection of that information, an employer then may be justified in not hiring the applicant on the basis that it does not have sufficient information to judge the applicant's suitability[249]—provided that it does not breach any applicable laws, such as anti-discrimination and equal employment opportunity laws.[250]

Location of privacy provisions concerning employee records

40.163 The recommended removal of the employee records exemption raises a further issue as to whether privacy provisions should be located in the *Privacy Act*, workplace relations legislation or elsewhere. At the time of the introduction of the private sector provisions of the *Privacy Act*, the Australian Government stated that privacy protection for employee records would be 'more properly a matter for workplace relations legislation'.[251] In contrast, the 2005 Senate Committee privacy inquiry concluded that the most appropriate place to protect employee privacy is in the *Privacy Act*, rather than in workplace relations legislation.[252]

40.164 Some stakeholders were of the view that the appropriate location for exemption would be in privacy legislation,[253] because this has worked well,[254] would allow users of the *Privacy Act* to assess their responsibilities and obligations properly, and would promote national consistency.[255] Some stakeholders suggested that the exemption should not be located in the *Workplace Relations Act* because that

---

249 See New Zealand Privacy Commissioner, 'It isn't Hard to be Fair …' (2005) 55 *Private Word* 4.

250 See, eg, *Disability Discrimination Act 1992* (Cth) s 15; *Anti-Discrimination Act 1977* (NSW) s 49D; *Anti-Discrimination Act 1991* (Qld) s 14.

251 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15752. See also Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 4, [109].

252 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.36]–[7.37], rec 13.

253 Retail Motor Industry, *Submission PR 407*, 7 December 2007 (endorsed by Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007); ACTU, *Submission PR 155*, 31 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

254 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.

255 UNITED Medical Protection, *Submission PR 118*, 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

legislation does not have universal application,[256] and relocating the exemption would raise unrelated workplace relations concerns.[257]

40.165 Other stakeholders argued that privacy regulation concerning employees' personal information should be addressed in workplace relations legislation,[258] including because employees' rights should be contained in a single legislative instrument that deals specifically with employment.[259] For example, AAPT Ltd submitted that all employee-related rights should be incorporated into a single legislative instrument, because separate legislative regimes and overlapping legislation (including state-based workplace surveillance and telecommunications interception legislation) created confusion and made the task of compliance onerous—'potentially lessening the protection that is otherwise afforded by the existence of these Acts'.[260] The Law Institute of Victoria stated that all aspects of workplace privacy should be regulated in one piece of legislation and a consistent approach should be adopted across states and territories.[261]

40.166 In the ALRC's view, the existence of the employee records exemption only increases the level of complexity of the *Privacy Act*. Introducing a further set of privacy principles in a different piece of legislation such as the *Workplace Relations Act* is unlikely to reduce the complexity of the privacy regime.[262]

40.167 Privacy protection of employee records should be located in the *Privacy Act* to allow maximum coverage of agencies and organisations and to promote consistency. Provisions regulating the privacy of employee records should not be located in workplace relations legislation because the *Workplace Relations Act* only applies to specified persons or entities, such as constitutional corporations and persons or entities that engage in constitutional trade and commerce.[263] In addition, employee records are

---

256 Retail Motor Industry, *Submission PR 407*, 7 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

257 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007.

258 Australian Business Industrial, *Submission PR 444*, 10 December 2007; Law Institute of Victoria, *Submission PR 200*, 21 February 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; AXA, *Submission PR 119*, 15 January 2007; UNITED Medical Protection, *Submission PR 118*, 15 January 2007; AAPT Ltd, *Submission PR 87*, 15 January 2007.

259 Law Institute of Victoria, *Submission PR 200*, 21 February 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; AXA, *Submission PR 119*, 15 January 2007; UNITED Medical Protection, *Submission PR 118*, 15 January 2007; AAPT Ltd, *Submission PR 87*, 15 January 2007.

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

261 Law Institute of Victoria, *Submission PR 200*, 21 February 2007.

262 See Australian Law Reform Commission, *Submission to the Australian Government Attorney-General's Department of Employment and Workplace Relations Review on Employee Records Privacy*, 8 April 2004.

263 The *Workplace Relations Act 1996* (Cth) only applies to specified persons or entities that employ, or usually employ, an individual. The specified persons or entities include: a constitutional corporation; the Australian Government; Australian Government authorities; a person or entity (which may be an unincorporated club) that employs (or usually employs), in connection with constitutional trade or

no different from other personal information and therefore should be regulated under the *Privacy Act* in the same way as other personal information.

commerce, an individual as a flight crew officer, a maritime employee, or a waterside worker; a body corporate incorporated in an Australian territory; and a person or entity (which may be an unincorporated club) that carries on an activity in an Australian territory in Australia: *Workplace Relations Act 1996* (Cth) s 6(1).

41. Political Exemption

Contents

Introduction

41.1 In Australia, as in other western countries, the major political parties compile sophisticated databases containing a great deal of information about the contact details, concerns and preferences of individual voters. This assists the parties in 'election planning, fundraising, advertising strategy and policy deliberation'.[1] The New Zealand Privacy Commissioner, Marie Shroff, reportedly has noted that businesses and governments increasingly rely on 'information-rich databases of personal information' in order to provide more efficient services and to market in a more targeted and effective manner.

> Political parties are no exception in hoping to gain extra mileage from collating and accessing details about voters and constituents.[2]

1 Canadian Press, 'Tory Database Draws Ire of Privacy Experts for Including Constituency Files', *CTV* (online), 18 October 2007, <www.ctv.ca>.

2 T Watkins, 'Voters Can Access Database Files', *Dominion Post* (online), 26 March 2007, <www.stuff .co.nz/dominionpost>.

41.2 Under s 90B of the *Commonwealth Electoral Act 1918* (Cth), the Australian Electoral Commission (AEC) provides (electronically) registered political parties, members of parliament (MPs), candidates for election and state and territory electoral authorities with information and certified lists of voters from the electoral rolls. This includes such details as name, address, age and occupation (optional). Under s 91A, such information may be used by politicians and political parties for a variety of 'permitted purposes', including: 'any purpose in connection with an election or referendum'; 'research regarding electoral matters'; 'monitoring the accuracy of information contained in a Roll'; and the performance by a senator or MP 'of his or her functions in relation to a person or persons enrolled' in the relevant electorate.

41.3 Information obtained under s 90B is 'protected information' under the Act,[3] and disclosure other than for a permitted purpose, or use for 'a commercial purpose', is an offence punishable by a fine of up to 1,000 penalty units.[4]

41.4 In addition to the raw data supplied by the AEC, political parties go to considerable lengths to augment the information:

> The ALP database is named Electrac, and the Liberal's is named Feedback. These databases use electronic White Pages to incorporate telephone numbers where available … Identifying voting preferences and issues of interest is a valuable albeit time consuming practice for political parties. Effective database management results in any contact by a constituent with an electorate office being logged into the system. Contact can be made by telephone, writing or in person … Door knocking, telephone canvassing and letters to the editor are additional methods by which information is gathered … Voter preferences recorded in the databases include swinging voter status, minor party or independent leaning, as well as strong or weak Liberal or Labor voter leanings. This information is most valuable in marginal seats.
>
> The information can be used for a number of purposes. Party organisations upload data from all electorates to track key issues and voting trends for use in qualitative polling, advertising and strategy formation. For individual MPs, the most important use is direct mail-outs targeted at swinging voters … Strongly Labor or Liberal Party identifying voters can be targeted for political donation.[5]

41.5 The *Privacy Act 1988* (Cth) does not apply to registered political parties or to political representatives engaging in certain activities 'in the political process'.[6] This exemption is usually referred to as the 'political exemption'. Australian Government ministers generally are required to comply with the *Privacy Act* only when they are acting in an official capacity. Parliamentary departments also are excluded from the operation of the Act.[7]

---

3 *Commonwealth Electoral Act 1918* (Cth) s 91A.

4 Ibid s 91B.

5 P van Onselen, 'Political Databases and Democracy: Incumbency Advantage and Privacy Concerns' (2004) *Democratic Audit of Australia* <democratic.audit.anu.edu.au>.

6 *Privacy Act 1988* (Cth) s 6C(1). Neither are political parties covered by the *Freedom of Information Act 1982* (Cth), since they are private organisations.

7 *Parliamentary Service Act 1999* (Cth) s 81(1)(a).

41.6 In this chapter, the ALRC examines the arguments for and against retention of the political exemption in the *Privacy Act*, and recommends—subject to relevant constitutional limitations—removal of this political exemption, as well as the exemptions applying to Australian Government ministers and parliamentary departments.

Exemption for registered political parties, political acts and practices

41.7 A 'registered political party'—defined as a political party registered under Part XI of the *Commonwealth Electoral Act*[8]—is specifically excluded from the definition of 'organisation' and, therefore, is exempt from the operation of the *Privacy Act*.[9] In addition, political acts and practices of certain organisations are exempt.[10] These organisations include:

- political representatives—namely, MPs and local government councillors;
- contractors and subcontractors of registered political parties and political representatives; and
- volunteers for registered political parties.[11]

41.8 Acts and practices covered by the exemption include those in connection with: elections held under an electoral law;[12] referendums held under a law of the Commonwealth, a state or a territory; and participation by registered political parties and political representatives in other aspects of the political process.[13] Some other Commonwealth laws also provide for the collection and use of personal information by registered political parties and political representatives.[14]

---

8 *Privacy Act 1988* (Cth) s 6(1). A list of registered political parties is available on the Australian Electoral Commission's website: Australian Electoral Commission, *Current List of Political Parties* (2007) <www.aec.gov.au/Parties_and_Representatives/Party_Registration/index.htm> at 6 May 2008.

9 *Privacy Act 1988* (Cth) s 6C(1).

10 Ibid ss 7(1)(ee), 7C.

11 Ibid s 7C.

12 An 'electoral law' means a Commonwealth, state or territory law relating to elections to a Parliament or to a local government authority: Ibid s 7C(6).

13 Ibid s 7C.

14 Under the *Do Not Call Register Act 2006* (Cth), registered political parties, independent MPs and electoral candidates are exempt from the prohibition against making unsolicited telemarketing calls to a number registered on the Do Not Call Register, provided the call is made for certain specified purposes. In addition, under the *Spam Act 2003* (Cth), registered political parties may, without the prior consent of the recipient, send 'designated commercial electronic messages'. Although these messages must include information about the authorising individual or organisation, they do not have to contain a functional unsubscribe facility.

41.9 In his second reading speech on the Privacy Amendment (Private Sector) Bill 2000 (Cth), the then Attorney-General, the Hon Daryl Williams AM QC MP, justified the exemption for political parties and political acts and practices on the basis of the importance of freedom of political communication to Australia's democratic process. He advised that the exemption was 'designed to encourage that freedom and enhance the operation of the electoral and political process in Australia'.[15]

41.10 On the other hand, at the time of the introduction of the Bill, Malcolm Crompton, the then Privacy Commissioner, stated that the exemption for political organisations was inappropriate. Rather, he stated that political institutions 'should follow the same practices and principles that are required in the wider community'.[16] These sentiments were echoed by Senator Natasha Stott Despoja, when she introduced a Private Member's Bill in June 2006 to remove the exemption for political acts and practices:[17]

> Politicians should be included in the rules that we expect the public and private sectors to abide by. We cannot lead and represent Australians when we do not adhere to the rules that we have made for them, as this merely plays into the notion that politicians cannot be trusted.[18]

Personal information handling in the political process

41.11 Personal information is handled in a number of facets of Australia's political process. Often, the use of this personal information will be associated closely with the system of representative democracy. For example, a constituent may write to his or her MP raising a problem or concern and, as a part of this correspondence, disclose personal information. In accordance with the MP's role as the constituent's representative, he or she may use or disclose the information by forwarding the correspondence on to the relevant minister or agency for response or by raising the matter in Parliament.

41.12 Where the individual to whom the information relates initiates this process, these information-handling practices generally will not be contentious. Concerns may arise, however, where a political representative uses or discloses personal information about a third party. This was illustrated in the case of *A v The United Kingdom*, in

---

15 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15753.

16 M Crompton (Federal Privacy Commissioner), 'Media Release: Federal Privacy Commissioner, Malcolm Crompton Comments on Private Sector' (Press Release, 12 April 2000).

17 Privacy (Extension to Political Acts and Practices) Amendment Bill 2006 (Cth). The Bill lapsed at the time the Australian Parliament was prorogued for the 2007 federal election. The Bill was reintroduced as Privacy (Extension to Political Acts and Practices) Amendment Bill 2006 [2008]. As at 9 May 2008, the Bill was before the Australian Senate.

18 Commonwealth, *Parliamentary Debates*, Senate, 22 June 2006, 19 (N Stott Despoja). The Australian Democrats also attempted unsuccessfully to introduce amendments to the Do Not Call Register Bill 2006 (Cth) to prevent politicians from making telemarketing calls: Commonwealth, *Parliamentary Debates*, Senate, 21 June 2006, 25 (N Stott Despoja). The *Do Not Call Register Act 2006* (Cth) is discussed in Ch 73.

which the applicant's MP, during a debate in the House of Commons, referred to the applicant and her children as 'neighbours from hell', as well as providing her name and address. The MP's remarks were widely publicised and ultimately engendered such hostility that it was necessary for the family to relocate.[19]

41.13 Further concerns relate to the use of electoral databases. As noted above, these are databases maintained by political parties that contain information on voters, which may include voters' policy preferences and party identification as well as such matters as the individual's occupation, membership of community organisations, and so on.[20] Privacy concerns arising from the existence and content of these databases include: political parties withholding from voters information they have stored; inaccurate information being stored on databases without giving voters the right to correct the record; political parties failing to inform voters that information is being compiled about them; and representatives of political parties failing to identify themselves appropriately when collecting information.[21]

41.14 The potential privacy implications of electoral databases recently were illustrated in Canada, when the Prime Minister's Office sent some households a greeting for Jewish New Year. Some recipients made complaints to the news media and their local MP, questioning both how their names came to be on such a mailing list and why a list of Jewish voters had been compiled.[22] The investigation by the Privacy Commissioner of Canada later was dropped because political parties are not governed by Canada's privacy laws.[23]

Relevant constitutional provisions

41.15 Any application of Australian privacy laws to political parties and agencies and organisations engaging in political acts and practices must take into account constitutional protections for some aspects of the political process. Of particular relevance are the constitutional doctrines of implied freedom of political communication and parliamentary privilege.

Implied freedom of political communication

41.16 The High Court of Australia has established that an essential element of representative democracy is the freedom of public discussion of political and economic

---

19 *A v The United Kingdom* [2002] ECHR 811.

20 P van Onselen and W Errington, 'Electoral Databases: Big Brother or Democracy Unbound?' (2004) 29 *Australian Journal of Political Science* 349, 349.

21 P van Onselen and W Errington, 'Suiting Themselves: Major Parties, Electoral Databases and Privacy' (2005) 20 *Australasian Parliamentary Review* 21, 28.

22 See: 'Privacy Commissioner Probes PM's List', *Toronto Star* (online), 11 October 2007, <www.thestar.com>.

23 'Privacy Czar Drops Rosh Hashanah Inquiry but Plans to Examine Party Databanks', *The Canadian Press* (online), 6 March 2008, <canadianpress.google.com>.

matters.[24] This freedom is not confined to election periods.[25] It does not confer, however, a personal right on individuals, but rather operates as a restriction on legislative and executive powers.[26] The freedom is not absolute,[27] and must be balanced against other public interests. In determining whether a law infringes the implied freedom of political communication, two questions must be answered:

> First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end …[28]

Parliamentary privilege

41.17 Parliamentary privilege refers to

> the sum of the peculiar rights enjoyed by each House collectively as a constituent part of the High Court of Parliament, and by Members of each House individually, without which they could not discharge their functions, and which exceed those possessed by other bodies or individuals.[29]

41.18 The freedom of speech and debate has been described as the single most important parliamentary privilege.[30] This privilege provides legal immunity to MPs for anything they may say or do in the course of parliamentary proceedings, or anything that is incidental to those proceedings.[31] In Australia, the *Parliamentary Privileges Act 1987* (Cth) provides a non-exhaustive definition of 'proceedings in parliament' for the purpose of freedom of speech and debate, being:

> all words spoken and acts done in the course of, or for purposes of or incidental to, the transacting of the business of a House or of a committee, and, without limiting the generality of the foregoing, includes:
>
> (a) the giving of evidence before a House or a committee, and evidence so given;
>
> (b) the presentation or submission of a document to a House or a committee;

---

24 *R v Smithers; Ex parte Benson* (1912) 16 CLR 99, 108, 109–110; *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1, 73; *Australian Capital Television Pty Ltd v Commonwealth (No 2)* (1992) 177 CLR 106, 232. The implied freedom of political communication is discussed in more detail in Ch 42.

25 *Cunliffe v Commonwealth* (1994) 182 CLR 272, 327; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 560–561.

26 *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 168; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.

27 *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1, 51, 76–77, 94–95; *Australian Capital Television Pty Ltd v Commonwealth (No 2)* (1992) 177 CLR 106, 142–144, 159, 169, 217–218; *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 126; *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211, 235; *Cunliffe v Commonwealth* (1994) 182 CLR 272, 336–337, 387; *Langer v Commonwealth* (1996) 186 CLR 302, 333–334; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.

28 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567.

29 *Erskine May's Treatise on the law, privileges, proceedings, and usage of Parliament*, cited in G Griffith, *Parliamentary Privilege: Major Developments and Current Issues* (2007) Parliament of New South Wales—Parliamentary Library, 2.

30 Parliament of United Kingdom—Joint Committee of the House of Lords and House of Commons, *Parliamentary Privilege—First Report* (1999), 26.

31 Ibid, 26.

> (c) the preparation of a document for purposes of or incidental to the transacting of any such business; and
>
> (d) the formulation, making or publication of a document, including a report, by or pursuant to an order of a House or a committee and the document so formulated, made or published.[32]

41.19 A further parliamentary privilege that potentially is relevant to the application of privacy law to the political process is the 'internal affairs privilege'—that is, the right for houses of parliament to administer their own internal affairs within parliamentary precincts. In the United Kingdom, this privilege has been interpreted to preclude the application of a number of statutes to the houses of parliament, including, among others, privacy laws.[33] The breadth of this interpretation, however, has been the subject of criticism. A Joint Committee of the House of Lords and House of Commons in the United Kingdom, for example, recommended that the internal affairs privilege should extend only to activities directly and closely related to proceedings in Parliament.[34] In the Australian context, Professor Enid Campbell has suggested that, in determining whether legislation can apply within parliamentary precincts, courts are likely to ask 'whether application of the statute to what occurs within parliamentary precincts impairs the capacity of a house to carry out its constitutional functions'.[35]

41.20 Parliament has powers to impose punishments for abuse of parliamentary privilege. Houses of parliament which judge their members to have abused the privilege of freedom of speech may suspend them from the service of the house for a period of time.[36] Under the *Parliamentary Privileges Act*, federal houses of parliament may impose penalties of imprisonment of up to six months for offences, and fines of up to $5,000 in the case of a natural person or $25,000 in the case of a corporation.[37]

41.21 The Senate and the House of Representatives also have passed resolutions implementing a 'right of reply' for citizens. These resolutions allow a person who has been referred to by name, or in such a way as to be identified readily, to make a submission claiming that he or she has been adversely affected by reason of that reference (including where the person's privacy has been unreasonably invaded) and request that an appropriate response is incorporated in the parliamentary record.[38] Most

---

32 *Parliamentary Privileges Act 1987* (Cth) ss 16(2).

33 See Parliament of United Kingdom—Joint Committee of the House of Lords and House of Commons, *Parliamentary Privilege—First Report* (1999), 83.

34 Ibid, 83.

35 E Campbell, *Parliamentary Privilege* (2003), 184. A purposive approach also was recently adopted by the Supreme Court of Canada in *Canada (House of Commons) v Vaid* [2005] ACWSJ 8082.

36 E Campbell, *Parliamentary Privilege* (2003), 55.

37 *Parliamentary Privileges Act 1987* (Cth) s 7.

38 The Australian Senate agreed to a right of reply procedure on 25 February 2988: J Odgers (ed) *Odgers' Australian Senate Practice* (11th ed, 2004), Appendix 2, [5]. The House of Representatives agreed to a resolution introducing a right of reply on 27 August 1997: Australian Parliament—House of Representatives Standing Committee of Privileges and Members' Interests, *Right of Reply* (2008) <www.aph.gov.au/house/committee> at 15 April 2008.

inquiries undertaken by the privileges committees in the House of Representatives and the Senate concern applications from persons seeking a right of reply.[39]

Government inquiries

41.22 In 2000, the Privacy Amendment (Private Sector) Bill was referred to the House of Representatives Standing Committee on Legal and Constitutional Affairs for inquiry and report (2000 House of Representatives Committee inquiry). The inquiry accepted that the exemption for political acts and practices seemed to be targeted at promoting the vitality and proper functioning of representative democracy. It suggested, however, that the exemption should be restricted to the participation of political representatives in parliamentary or electoral processes, rather than in other aspects of the political process.[40] The Australian Government rejected the recommendation on the basis that this would narrow significantly the scope of the exemption.[41]

41.23 The 2000 House of Representatives Committee inquiry also recommended that the *Privacy Act* should be amended to provide that the exemption does not permit political parties or political representatives to sell or disclose personal information collected in the course of their duties to anyone not covered by the exemption.[42] The Australian Government rejected this recommendation on the basis that the exemption would not apply unless the personal information was being sold or disclosed for the purpose of an election, a referendum or participation in another aspect of the political process.[43] A note was inserted in the Bill, however, to make it clear that the exemption does not extend to the use or disclosure (by way of sale or otherwise) of personal information collected by virtue of the exemption in a way that is not covered by the exemption.[44]

---

39 Of the 13 Reports issued by the Senate Committee of Privileges between November 2004 and October 2007, seven were applications from individuals seeking a right of reply. Parliament of Australia—Senate, *Senate Privileges Committee—Completed Inquiries* (2008) <www.aph.gov.au/Senate> at 30 April 2008. Of the six Reports issued by the House of Representatives Standing Committee of Privileges between November 2004 and October 2007, four were applications from individuals seeking a right of reply. Parliament of Australia—House of Representatives, *Standing Committee of Privileges—Committee Activities (Inquiries and Reports)* (2008) <www.aph.gov.au/house> at 29 April 2008.

40 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), recs 11, 12.

41 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

42 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), rec 13.

43 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

44 Further Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [1]; *Privacy Act 1988* (Cth), note to s 7C.

41.24 In 2005, the Senate Legal and Constitutional References Committee reviewed the private sector provisions of the *Privacy Act* (Senate Committee privacy inquiry).[45] A number of submissions to the Senate Committee privacy inquiry objected strongly to the exemption for political acts and practices.[46] The Senate Committee privacy inquiry concluded that the exemption in relation to political acts and practices was problematic and recommended that it should be examined by the ALRC as part of its wider review of the *Privacy Act*.[47]

International instruments and laws

41.25 The European Union (EU) *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) contains a specific exemption allowing the compilation of data by political parties on people's political opinions in the course of electoral activities, provided that appropriate safeguards are established.[48] Under the EU Directive, the processing of data by political organisations for marketing purposes also is permitted, subject to certain conditions.[49]

41.26 The Asia-Pacific Economic Cooperation (APEC) Privacy Framework does not contain a specific exemption or exception concerning political or electoral activities. The Explanatory Memorandum to the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD) states that exceptions to the privacy principles are to be limited to those that are 'necessary in a democratic society'.[50]

41.27 A number of comparable overseas jurisdictions, including the United Kingdom, New Zealand and Hong Kong, do not exempt political parties or political acts and practices from the operation of their information privacy legislation. As noted above, political parties are not caught by federal privacy legislation in Canada, but some parties—namely the Liberal Party and the New Democratic Party—say that they voluntarily comply with the privacy principles, only collect and retain personal information with the consent of the individual concerned, and allow an individual to see his or her file upon request.[51]

---

45 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

46 Ibid, [4.87]–[4.94].

47 Ibid, [7.29]–[7.30], rec 11.

48 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recital 36.

49 Ibid, recital 30.

50 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [47].

51 Canadian Press, 'Tory Database Draws Ire of Privacy Experts for Including Constituency Files', *CTV* (online), 18 October 2007, <www.ctv.ca>.

41.28 In September 2005, an international conference of privacy and data protection commissioners adopted a *Resolution on the Use of Personal Data for Political Communication*. The Resolution states that any processing of personal data for the purposes of political communication must respect the fundamental rights and freedoms of interested persons and must comply with specific data protection principles. In particular, the Resolution provides that certain principles concerning the collection of personal data, data quality and security, rights of access and correction, and the right to opt out of unsolicited communication should be observed in political communication. In addition, the Resolution recommends that the processing of personal data should be based on the individual's consent or another legitimate ground provided for by the law.[52]

Submissions and consultations

41.29 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the exemption in the *Privacy Act* should be removed for registered political parties[53] and political acts and practices.[54] There was considerable support for removing these exemptions.[55] Some stakeholders suggested, for example, that preferential treatment of registered political parties—by exempting them from compliance with the *Privacy Act*—undermines public trust in the political process.[56] Stakeholders also were concerned that: political parties can collect information about constituents from third parties that could be inaccurate;[57] and constituents do not know what information was collected by the parties and have no right of access to, or correction of, personal information in electoral databases.[58]

---

52 *Resolution on the Use of Personal Data for Political Communication (Adopted at the 27th International Conference on Privacy and Personal Data Protection, Montreux, 14–16 September 2005)* (2005) <www.privacyconference2005.org> at 6 May 2008.

53 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–7.

54 Ibid, Question 5–8.

55 For political parties, see 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; New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007; Confidential, *Submission PR 134*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; K Pospisek, *Submission PR 104*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007. For political acts and practices, see 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; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Royal Women's Hospital Melbourne, *Submission PR 108*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007.

56 See, eg: Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007; B Such, *Submission PR 71*, 2 January 2007.

57 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

58 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Confidential, *Submission PR 134*, 19 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

41.30 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that:

- the exemption in the *Privacy Act* for registered political parties and political acts and practices should be removed;[59] and

- the *Privacy Act* should be amended to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.[60]

Removing the political exemption

41.31 Many stakeholders supported removing the political exemption.[61] The Cyberspace Law and Policy Centre, for example, submitted that:

> Most individuals, if they were aware of the increasingly sophisticated database operations of political parties, would see them as one of the clearest examples of information processing that needs the protection of the privacy principles.[62]

41.32 Liberty Victoria provided the example of a Victorian senator who had passed the medical records of a woman who had sought an abortion to the media. It submitted that, in light of this conduct, the *Privacy Act* should apply across all sectors, including elected representatives.[63]

41.33 Several stakeholders expressed the view that removing the political exemption would improve the operation of the democratic process.[64] The Office of the Victorian Privacy Commissioner (OVPC), for example, endorsed the views of the previous Victorian Privacy Commissioner, Paul Chadwick, that 'one aspect of trust [in public institutions] is the willingness to submit to the same levels of accountability as everybody else'.[65] The Public Interest Advocacy Centre (PIAC) noted:

> The unregulated operation of [electoral] databases can diminish public confidence in the democratic process, discourage constituents from contacting their local Member of Parliament about issues of concern, and distort the political process by skewing it in favour of swinging voters. The proposal to remove the exemption should result in

---

59 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 37–1.

60 Ibid, Proposal 37–2.

61 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; Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Confidential, *Submission PR 535*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007; Rev B Harris, *Submission PR 321*, 14 September 2007.

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

63 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.

64 See, eg, Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

65 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

> greater transparency and accountability in the way that political parties and their representatives handle personal information.[66]

41.34 The Office of the Privacy Commissioner (OPC) advised that it receives very few complaints or inquiries about the political exemption, although this fact is ambiguous. It may mean that the *Privacy Act* provides an appropriate balance; the OPC noted, on the other hand, that the low frequency of complaints also may be a result of individuals not being aware of how political parties handle their personal information. The OPC submitted that, if the political parties exemption is to be retained,

> political parties should be required to comply with a few key privacy principles that will provide individuals with transparency and protection regarding how political parties handle their information. These key principles include the openness principle, NPP 5, and the access and correction principle, NPP 6.[67]

41.35 Some stakeholders also commented on the importance of applying specific privacy principles to registered political parties and political acts and practices, including the: 'Openness' principle;[68] 'Access and Correction' principle;[69] and 'Data Security' principle.[70]

41.36 The Australian Labor Party (ALP) was the only registered political party that made a submission to this Inquiry.[71] The ALP commented that the current law operates effectively to promote political communication, while protecting the privacy of individuals from commercial and other intrusions. The ALP submitted that

> the exemption for registered political parties under the *Privacy Act* is essential to the conduct of election campaigns and facilitates the effective communication of the policies, ideas and visions which underpin our democratic processes.[72]

41.37 The ALP suggested that the current law on registration of political parties under Part XI of the *Commonwealth Electoral Act* provides an effective and practical way to ensure that private information disclosed under the political exemption is treated appropriately.[73]

---

66 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

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

68 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

69 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

70 Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540,* 21 December 2007.

71 In October 2006, the ALRC wrote to the Liberal Party of Australia, the ALP, the National Party of Australia, the Country Liberal Party, the Australian Democrats, the Australian Greens, and the Family First Party. In October 2007, the ALRC corresponded with the Liberal Party of Australia and the ALP to request consultation meetings. The ALRC also consulted with Senator Natasha Stott Despoja, who advised that the Australian Democrats supported the removal of the political exemption: N Stott Despoja, *Consultation*, Canberra, 21 March 2007.

72 Australian Labor Party, *Submission PR 486,* 18 December 2007.

73 Ibid. Requirements for registration of a political party under the *Commonwealth Electoral Act* include having: at least one member who is a member of the Parliament of the Commonwealth or, otherwise, at least 500 members; and a written constitution in place setting out the aims of the party.

41.38 The Right to Know Coalition did not support the ALRC's proposal that the political exemption be removed on the basis that this might adversely effect the media's ability to report on matters affecting the political process. The Coalition argued that the 'adversarial' nature of Australian politics means that 'journalists often receive information from one party about the other that would fall within the definition of personal information'. The Coalition submitted that—if any change were to occur to the exemption for political parties—the exemption should be modified only to the extent of imposing obligations of: notification; data quality and security; and access and correction. The Coalition also suggested that the disclosure of information by political parties should be protected by a defence of qualified privilege, similar to that which applies under defamation law.[74]

Accommodating the relevant constitutional doctrines

41.39 Most stakeholders that commented on the proposal supported amending the *Privacy Act* to clarify that it does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.[75] The OPC noted, for example, that including such a provision would be consistent with similar provisions in legislation such as the *Spam Act 2003* (Cth) and the *Telecommunications Act 1997* (Cth).[76]

41.40 The ALP expressed concerns, however, that including a definition based on the implied freedom of political communication could result in legal challenges to a range of activities by political parties, which would be detrimental to the political process.[77] The Right to Know Coalition submitted that applying the implied constitutional doctrine of freedom of political communication to the *Privacy Act* could be difficult because of the 'developing and relatively unclear jurisprudence' surrounding the doctrine.[78]

Options for reform

41.41 There are compelling policy reasons—as well as strong stakeholder support—for applying privacy obligations to registered political parties and political acts and practices. However, any lessening of the scope of the political exemption must take into account the strong public interest in promoting Australia's system of representative democracy. The ALRC has identified three options for balancing these competing interests:

---

74 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

75 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. The Australian Direct Marketing Association did not disagree with the proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

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

77 Australian Labor Party, *Submission PR 486*, 18 December 2007.

78 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

- removing the political exemption, subject to the relevant constitutional limitations;

- providing limited exceptions to—rather than exemptions from—the *Privacy Act* for registered political parties and political acts and practices; and

- requiring registered political parties and other entities engaging in political acts and practices to develop information-handling guidelines, in consultation with the OPC.

Removal of political exemption, subject to relevant constitutional limitations

41.42 The most direct way of balancing the public interest in protecting individuals' information privacy and the constitutional protections directed towards promoting representative democracy would be to remove the political exemption, subject to the extent (if any) that it conflicts with relevant constitutional protections. Most relevantly, these protections involve the doctrine of implied freedom of political communication and parliamentary privilege. This was the approach proposed by the ALRC in DP 72.

41.43 Arguably, even in the absence of specific legislative provisions, the *Privacy Act* would be interpreted in a way that is consistent with any relevant constitutional limitations. In particular, s 15A of the *Acts Interpretation Act 1901* (Cth) provides that:

> Every Act shall be read and construed subject to the Constitution, and so as not to exceed the legislative power of the Commonwealth, to the intent that where any enactment thereof would, but for this section, have been construed as being in excess of that power, it shall nevertheless be a valid enactment to the extent to which it is not in excess of that power.

41.44 The High Court, however, has upheld a number of limitations to the effectiveness of the above provision of the *Acts Interpretation Act*. These include: where a provision of general application can be read down in a number of possible ways and it is unclear upon which head of legislative power Parliament is relying;[79] and where it is unclear whether a provision of general application is intended to have a distributive operation. The latter limitation refers to whether a particular requirement is intended to apply to each and every person within a class independently of its application to others; or whether 'all were intended to go free unless all were bound'.[80]

41.45 The Office of Parliamentary Counsel has issued a model provision for an Act to be read down so that it does not infringe the constitutional doctrine of implied freedom of political communication. The provision reads:

---

79 See, eg, *Strickland v Rocla Concrete Pipes Ltd* (1971) 124 CLR 468.

80 See *R v Poole; Ex Parte Henry (No 20)* (1939) 61 CLR 364, 652. Limitations to severability are discussed in Australian Government Office of Parliamentary Counsel, *Drafting Direction No 3.1—Constitutional Law Issues* (2006).

> This Act does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication.[81]

41.46 Equivalent provisions are contained in several pieces of Commonwealth legislation, including the *Spam Act*, the *Do Not Call Register Act*, the *Criminal Code Act 1995* (Cth) and the *Telecommunications Act*.[82]

41.47 Some Commonwealth laws also include provisions expressly preserving parliamentary privileges.[83] Section 10 of the *Evidence Act 1995* (Cth), for example, provides:

> (1) This Act does not affect the law relating to the privileges of any Australian Parliament or any House of any Australian Parliament.
>
> (2) In particular, subsection 15(2) [compellability to give evidence] does not affect, and is in addition to, the law relating to such privileges.

41.48 The question of whether the application of the *Privacy Act* to a specific act or practice would infringe a relevant constitutional doctrine would be determined on a case-by-case basis by the relevant court or tribunal.

Exceptions to specific privacy principles

41.49 An alternative approach would be to provide registered political parties and agencies and organisations engaging in political acts and practices with exceptions to specific privacy principles. This approach involves identifying the particular privacy principles that could conflict with Australia's system of representative democracy.

41.50 The *Resolution on the Use of Personal Data for Political Communication*, discussed above, provides that political communication should observe privacy principles relating to the collection of personal data, data quality and security, rights of access and correction, and the right to opt out of unsolicited communication.[84]

41.51 As noted above, some stakeholders also made submissions to this Inquiry suggesting particular privacy principles that should apply to registered political parties and political acts and practices. These include the 'Openness' principle, the 'Access and Correction' principle, and the 'Data Security' principle.

---

81 Australian Government Office of Parliamentary Counsel, *Drafting Direction No 3.1—Constitutional Law Issues* (2006), [8].

82 *Spam Act 2003* (Cth) s 44; *Do Not Call Register Act 2006* (Cth) s 43; *Criminal Code Act 1995* (Cth) s 102.8(6); *Telecommunications Act 1997* (Cth) s 138. See also *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS(13); *Broadcasting Services Act 1992* (Cth) s 61BG; *Olympic Insignia Protection Act 1987* (Cth) s 73; *Interactive Gambling Act 2001* (Cth) s 61BB(4).

83 *Evidence Act 1995* (Cth) s 10; Public Interest Disclosures Bill 2007 (Cth) s 6.

84 *Resolution on the Use of Personal Data for Political Communication (Adopted at the 27th International Conference on Privacy and Personal Data Protection, Montreux, 14–16 September 2005)* (2005) <www.privacyconference2005.org> at 6 May 2008.

Development of information-handling guidelines

41.52 Another option for reform is to retain the political exemption, on the condition that registered political parties, and other entities engaging in political acts and practices, are subject to information-handling guidelines.

41.53 In Victoria, for example, MPs are exempt from the *Information Privacy Act 2000* (Vic).[85] During the passage of the Act, however, there was bipartisan agreement that MPs should be covered by self-imposed standards.[86] The Victorian Scrutiny of Acts and Regulations Committee, in consultation with information privacy consultants, has developed a *Privacy Code of Conduct for Members of the Victorian Parliament*. The Code sets out seven privacy principles for MPs, including: collection; use and disclosure; data quality; data security; openness; access and correction; and accountability.[87] However, the Code has not yet been implemented by either of the Victorian Houses of Parliament.

ALRC's view

Removing the political exemption

41.54 In the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. Unless there is a sound policy reason to the contrary, political parties and agencies and organisations engaging in political acts and practices should be required to handle personal information in accordance with the requirements of the *Privacy Act*.

41.55 The most compelling reason for exempting registered political parties and agencies and organisations engaging in political acts and practices from the *Privacy Act* is the need to recognise the special status of political acts and practices under the *Australian Constitution*. In Chapter 42, for example, the ALRC justifies retention of the journalism exemption on the basis that there is a compelling public interest in freedom of expression and in allowing the free flow of information required to sustain the vitality of democratic institutions.

41.56 The ALRC is not convinced, however, that all (or even the majority) of information-handling activities undertaken by registered political parties and those engaged in political acts and practices warrant legislative immunity. In particular, registered political parties and those engaging in political acts and practices should:

---

85 *Information Privacy Act 2000* (Vic) s 9(1). MPs are subject, however, to the *Health Records Act 2001* (Vic).

86 Parliament of Victoria—Scrutiny of Acts and Regulations Committee, *Final Report on a Privacy Code of Conduct for Members of the Victorian Parliament* (2002), 1.

87 Ibid.

- collect information by lawful and fair means; ensure the quality and security of the information;
- set out their policies on the management of personal information;
- let individuals know what personal information is held about them; and
- allow individuals the right to access and correct such information.

41.57 Compliance with these information-handling practices by those agencies and organisations engaging in the political process will promote—rather than impede—public confidence in the democratic process. Similarly, there is an argument that exempting political parties entrenches the advantages of incumbency, contrary to the best interests of representative democracy.[88]

41.58 A further justification put forward for retaining the political exemption was that the application of the *Privacy Act* to registered political parties is unnecessary because adequate protection already is in place. In particular, the ALP suggested that protection is afforded by the requirements for registration under the *Commonwealth Electoral Act*.

41.59 Registration requirements do not provide directly for privacy protections. All that is required for a party to be eligible for registration under the *Commonwealth Electoral Act* is that it has: at least one member who is a member of the Parliament of the Commonwealth or, otherwise, at least 500 members; and a written constitution in place setting out the aims of the party. The legislation does not specify any provisions that should be included in a party's constitution, including any requirement for the party to protect privacy when handling personal information.[89]

41.60 As noted above, houses of parliament have significant powers to impose punishments on their members for abuse of parliamentary processes. These powers do not extend, however, to the broader information-handling practices of registered political parties and those engaging in political acts and practices.

41.61 In the ALRC's view, political parties and those engaging in political acts and practices should be subject to the *Privacy Act*—provided that the legislation can accommodate adequately the constitutional doctrines of implied freedom of political communication and parliamentary privilege. Removing the political exemption also accords with a number of comparable overseas jurisdictions, which do not exempt political parties or those engaging in political acts and practices from complying with privacy legislation, including the United Kingdom, New Zealand and Hong Kong.

---

88 P van Onselen, 'Political Databases and Democracy: Incumbency Advantage and Privacy Concerns' (2004) *Democratic Audit of Australia* <democratic.audit.anu.edu.au>.

89 *Commonwealth Electoral Act 1918* (Cth) s 123(1).

41.62 The recommended removal from the *Privacy Act* of the political exemption is not intended to displace more specific legislation that permits the collection and use of personal information by registered political parties and political representatives, including the *Commonwealth Electoral Act*, the *Do Not Call Register Act* and the *Spam Act*.

Accommodating the relevant constitutional doctrines

41.63 Any narrowing of the political exemption must take into account the constitutional doctrines of parliamentary privilege and the implied freedom of political communication. Precluding the application of the *Privacy Act* to acts and practices falling within parliamentary privilege or the freedom of political communication is the preferable approach. This allows a targeted and nuanced approach to balancing the potential conflicts between the requirements for handling personal information in a way that respects personal privacy and the exchange of personal information necessary for a representative democracy.

41.64 For example, assume that an individual discloses personal information to his or her MP in order to seek assistance with a problem. The MP could disclose the information in a number of ways, including to a relevant minister or agency, or in the course of parliamentary proceedings. These disclosures generally would fall within the relevant constitutional protections and, therefore, the requirements under the *Privacy Act* would not apply. Where the MP enters the personal information into an electoral database for the purpose of party fundraising, however, this use or disclosure may not fall within the doctrines of parliamentary privilege and the implied freedom of political communication. Consequently, if the ALRC's recommendation is implemented, the MP would be required to comply with the requirements under the *Privacy Act*.

41.65 In order to promote certainty about the application of the *Privacy Act* to registered political parties and political acts and practices, the ALRC recommends that the OPC should provide guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the *Privacy Act*.[90]

Alternative options for reform

41.66 Other options are available to balance the public interest in protecting individuals' information privacy with the personal information-handling practices incidental to a representative democracy.

41.67 Political parties and those engaging in the political process could be required to comply only with specific privacy principles. In particular, these could include: the 'Openness' principle; the 'Data Quality' principle; the 'Data Security' principle; and the 'Access and Correction' principle. Arguably, this approach may provide more certainty to those engaging in the political process about how the *Privacy Act* will be

90 Rec 41–3.

applied to their acts and practices. In the ALRC's view, however, setting out specific exceptions to the privacy principles is a blunt tool to classify the particular acts and practices that warrant immunity from the requirements of the *Privacy Act*. OPC guidance to registered political parties and others should provide sufficient certainty.

41.68 Another option for reform is for political parties and others engaging in political acts and practices to develop guidelines for their handling of personal information. There are few avenues, however, to implement and enforce such guidelines. Accordingly, this reform has limited capacity to address the privacy concerns arising out of personal information handling in the political process.

41.69 In the event that the current political exemption remains, however, guidelines for personal information handling in the political process would provide individuals with a minimum level of privacy protection. In particular, transparent information-handling practices allow an individual to make more informed decisions about his or her participation in the political process—for example, the amount of personal information that he or she chooses to disclose to his or her MP. These information-handling guidelines should be developed in consultation with the OPC. The guidelines also could be informed by the voluntary code of conduct for Victorian MPs developed by the Victorian Parliament's Scrutiny of Acts and Regulations Committee.[91]

Ministers

41.70 The *Privacy Act* applies to Australian Government ministers only to the extent that their acts and practices relate to the affairs of agencies, 'eligible case managers'[92] or 'eligible hearing service providers';[93] or where the acts and practices are in relation to a record concerning these affairs that is in the ministers' possession in their official capacity.[94] Other acts and practices of ministers are exempt from the operation of the Act.[95]

---

91 Parliament of Victoria—Scrutiny of Acts and Regulations Committee, *Final Report on a Privacy Code of Conduct for Members of the Victorian Parliament* (2002).

92 The Information Privacy Principles (IPPs) apply to the acts and practices of 'eligible case managers' in connection with the provision of case management services or the performance of their functions under the *Employment Services Act 1994* (Cth): *Privacy Act 1988* (Cth) ss 6(1), 7(1)(cb). An 'eligible case manager' is an entity that is or has been a contracted case manager within the meaning of the *Employment Services Act*: *Privacy Act 1988* (Cth) s 6(1). Although the *Employment Services Act* was repealed in April 2006, the *Privacy Act 1988* (Cth) continues to provide privacy protection in relation to acts and practices of entities that have been eligible case managers.

93 The IPPs apply to the acts and practices of 'eligible hearing service providers' in connection with the provision of hearing services under an agreement made under pt 3 of the *Hearing Services Administration Act 1997* (Cth): *Privacy Act 1988* (Cth) ss 6(1), 7(1)(cc). An 'eligible hearing service provider' means an entity that is, or has been, engaged under pt 3 of the *Hearing Services Administration Act* to provide hearing services: *Privacy Act 1988* (Cth) s 6(1).

94 *Privacy Act 1988* (Cth) s 7(1)(d)–(ed).

95 Ibid s 7(1)(a)(iii).

41.71 There is no exemption for government ministers from privacy legislation in the United Kingdom, Italy, New Zealand or Hong Kong. In Victoria and Tasmania, privacy legislation expressly applies to government ministers.[96]

41.72 The OPC observed that the formulation of the exemption applying to Australian Government ministers is complex:

> In the *Privacy Act* under s 6(1), a Minister is defined as an 'agency' and is therefore covered by the Act, however, his or her acts are excluded from coverage of the *Privacy Act* under s 7(1)(a)(iii). However, a Minister acting in his or her official capacity in relation to agencies within his or her portfolio are covered under ss 7(1)(d), (e), (ea), (eb), (ec), and (ed). … to help reduce this complexity, the definition of 'agency' which currently includes a Minister, should add words that describe the specific acts and practices of the Minister that are covered.[97]

41.73 In addition, it was said that the exemption is difficult to apply. As discussed above, ministers acting in their official capacity are bound by the *Privacy Act*, while MPs engaging in political acts and practices are not. The OVPC submitted that:

> It is sometimes difficult to determine in what capacity a Minister acts—in their Ministerial capacity or in their capacity as an elected Member of Parliament—when personal information is collected and disclosed, at times under the umbrella of Parliamentary immunity. It is also unclear whether Ministerial advisors are subject to privacy obligations, given the nature of their employment and principles of ministerial accountability.[98]

41.74 One individual submitted that the exemption applying to ministers results in 'a danger that the information they hold will be used for political purposes and not for the benefit of the individual or the safety of the nation'.[99]

41.75 In DP 72, the ALRC proposed that the partial exemption that applies to Australian Government ministers should be removed from the *Privacy Act*.[100] This proposal was supported by a broad range of stakeholders.[101]

---

96 *Information Privacy Act 2000* (Vic) s 9(1)(a); *Personal Information Protection Act 2004* (Tas) s 3 (definition of 'public sector body').

97 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

98 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

99 K Handscombe, *Submission PR 89*, 15 January 2007.

100 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 37–1(c).

101 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; Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Confidential, *Submission PR 535*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007.

ALRC's view

41.76 Currently, Australian Government ministers acting in their official capacity are subject to the *Privacy Act*. For the reasons underlying the recommended removal from the *Privacy Act* of the political exemption, there is no sound policy basis for exempting ministers when they are *not* acting in their official capacity, unless they fall within another exemption from the Act.[102] Accordingly, the partial exemption that applies to Australian Government ministers should be removed.

Recommendation 41–1 The *Privacy Act* should be amended to remove the exemption for registered political parties and the exemption for political acts and practices by:

(a) deleting the reference to a 'registered political party' from the definition of 'organisation' in s 6C(1) of the Act;

(b) repealing s 7C of the Act; and

(c) removing the partial exemption that is currently applicable to Australian Government ministers in s 7(1) of the Act.

Recommendation 41–2 The *Privacy Act* should be amended to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege.

Parliamentary departments

41.77 Parliamentary departments include the Department of the Senate, the Department of the House of Representatives and the Department of Parliamentary Services (DPS).[103] The Department of the Senate and the Department of the House of Representatives provide advice and support to the Senate and the House of Representatives respectively, and to committees, senators and members.[104] The DPS is responsible for providing information, analysis and advice to the Australian Parliament, maintaining and facilitating access to the Parliamentary Library's electronic and print information resources and providing a range of other services, such as information technology, broadcasting and Hansard services.[105] Secretaries of the

102 For example, when they are handling personal information as individuals in the context of their personal, business or household affairs.

103 *Parliamentary Service Act 1999* (Cth) s 54. The DPS is a Department of the Parliament established by resolutions passed by each House of the Australian Parliament: Australian Parliamentary Service Commissioner, *Annual Report 2004–05* (2005), App A.

104 Australian Parliamentary Service Commissioner, *Annual Report 2006–07* (2007), 6.

105 Ibid, 6.

Department of the Senate, the Department of the House of Representatives and the DPS have roles and responsibilities similar to those of agency heads of the Australian Public Service.[106]

41.78 The Presiding Officers of the Parliament—the President of the Senate and the Speaker of the House of Representatives[107]—are responsible for the administration of the three parliamentary departments. This role has been likened to the role of a Minister in relation to a department of state.[108] An independent Parliamentary Service Commissioner provides advice to Presiding Officers of both Houses of Parliament on the management policies and practices of the Parliamentary Service, and, if requested by the Presiding Officers, may inquire into and report on matters relating to the Parliamentary Service that are specified in the request.

41.79 The Office of the Parliamentary Librarian is an office within the DPS. The main function of the Parliamentary Librarian is to provide information, research, analysis and advice to senators and members of the House of Representatives in support of their parliamentary and representational role.[109]

Application of the *Privacy Act* to parliamentary departments

41.80 Section 81(1)(a) of the *Parliamentary Service Act 1999* (Cth) provides that, in any Act other than the *Privacy Act*, a reference to an 'agency' includes a reference to a Department of the Parliament established under the *Parliamentary Service Act*. Since Departments of the Parliament established under the *Parliamentary Service Act* fall outside the definition of an 'agency' under the *Privacy Act*, they are exempt from the operation of the *Privacy Act*.

41.81 There is no reference to the exemption in either the *Privacy Act* or the *Public Service Act*, from which the *Privacy Act* derives its definition of a department. The secondary legislative materials relating to the *Parliamentary Service Act* do not disclose a policy justification for the exemption of the parliamentary departments from the *Privacy Act*.

41.82 The application of the *Privacy Act* to parliamentary departments will be affected by the constitutional doctrine of parliamentary privilege, discussed above. For example, parliamentary departments conduct a number of activities that fall within the freedom of speech and debate. These could include, for example: the preparation of a document for the purposes of, or incidental to, the transacting of parliamentary business';[110] and the formulation, making or publication of a document, including a report, by or pursuant to an order of a House or committee and the document so

106 Ibid, 7.
107 *Parliamentary Service Act 1999* (Cth) s 7.
108 Australian Parliamentary Service Commissioner, *Annual Report 2006–07* (2007), 1.
109 *Parliamentary Service Act 1999* (Cth) ss 38A, 38B.
110 *Parliamentary Privileges Act 1987* (Cth) s 16(2)(c).

formulated, made or published.[111] Furthermore, the 'internal affairs privilege' could, in exceptional circumstances, extend to the management and administration of parliamentary departments.[112]

Submissions and consultations

41.83 In DP 72, the ALRC asked whether the parliamentary departments should continue to be exempt from the *Privacy Act* and, if so, what should be the scope of the exemption.[113]

41.84 In consultations with the ALRC, the parliamentary departments advised that they were not aware of a policy justification for this exemption, beyond the requirements of parliamentary privilege.[114] PIAC and the Cyberspace Law and Policy Centre submitted that there was no policy justification for parliamentary departments to continue to be exempt from the *Privacy Act*.[115] The Australian Privacy Foundation also supported the removal of the exemption.[116]

41.85 The OPC did not provide a specific view on whether the parliamentary departments should continue to be exempt from the operation of the *Privacy Act*. It commented, however, that 'there should be a clear public interest enunciated for any exception to be maintained'. The OPC noted that, if these bodies are to be exempt from the operation of the *Privacy Act*:

- any exemption should be explicitly referred to in the *Privacy Act*;
- exemptions should be included in a schedule to the Act; and
- all entities that are not covered by the *Privacy Act* should implement and make publicly available a set of standards for the handling of personal information.[117]

ALRC's view

41.86 Beyond the requirements of the constitutional protections for the political process, the ALRC is not aware of any policy justification for exempting parliamentary departments from the operation of the *Privacy Act*. This position was supported by the

---

111 Ibid s 16(2)(d).

112 The Joint Committee of the House of Lords and House of Commons in the United Kingdom advised, however, that 'management functions related to the provision of services in either House are only exceptionally subject to privilege'. The Report went on to note that—when management is dealing with matters directly related to proceedings within the scope of the freedom of speech and debate—the management and administration of House departments are not generally subject to privilege: Parliament of United Kingdom—Joint Committee of the House of Lords and House of Commons, *Parliamentary Privilege—First Report* (1999), 83.

113 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 34–2.

114 Departments of the Senate, House of Representatives and Parliamentary Services, *Consultation PC 183*, Canberra, 22 October 2007.

115 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

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

parliamentary departments themselves. Accordingly, the ALRC is of the view that the *Privacy Act* should apply to the parliamentary departments. As recommended, above, the Act will be subject to the implied constitutional doctrines of freedom of political communication and parliamentary privilege.

Recommendation 41–3 Parliamentary departments should be included within the definition of 'agency' in the *Privacy Act* by removing the words 'other than the *Privacy Act 1988*' from section 81(1) of the *Parliamentary Services Act 1999* (Cth).

Guidance on applying the *Privacy Act* to the political process

41.87 In DP 72, the ALRC proposed that, before the removal of the political exemption comes into effect, the OPC should provide guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the *Privacy Act*.[118]

41.88 Stakeholders supported the provision of guidance from the OPC.[119] The OPC agreed that, should the exemptions for political parties and political acts and practices be removed, additional guidance would be required. It noted, however, that this would require appropriate resources.[120] The OVPC suggested that the guidance should be developed jointly by, or in consultation with, state and territory privacy commissioners.[121]

41.89 PIAC suggested that removing the political exemption should not be contingent on the provision of support and advice from the OPC. It commented that postponing the removal of the exemption until such guidance was developed and published might lead to an indefinite delay. PIAC suggested, therefore, that a specific time frame for removing the exemption should be set out in the legislation.[122]

ALRC's view

41.90 The OPC should provide guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the *Privacy Act*. In particular, this guidance will help to provide certainty to agencies and organisations on

---

118 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 37–3.

119 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. The Australian Direct Marketing Association did not disagree with the proposal for OPC guidance: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

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

121 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

122 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

the interaction between the requirements under the *Privacy Act* and the constitutional doctrines of implied freedom of political communication and parliamentary privilege.

41.91 In Chapter 45, the ALRC considers the role of the OPC in implementing this Report's recommendations. The ALRC notes that the OPC should develop and publish the guidance documents recommended in this Report in a timely manner. The timeframe in which the OPC can provide guidance on the application of the *Privacy Act* to the political process, however, will depend on the resource levels provided to the OPC, and other competing priorities. The ALRC, therefore, does not recommend a specific timeframe in which this guidance should be provided.

Recommendation 41–4 Before the removal of the exemptions for registered political parties and for political acts and practices from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act.

42. Journalism Exemption

Contents

Introduction

42.1 Acts done and practices engaged in by media organisations in the course of journalism are exempt from the operation of the *Privacy Act 1988* (Cth), provided the organisation meets certain requirements, including being publicly committed to standards that deal with privacy. This exemption promotes the public interest in freedom of expression and the free flow of information critical to the maintenance of a democratic society. Some concerns have been raised, however, about the nature and operation of the exemption, including the:

- broad scope of the exemption;
- lack of criteria and independent assessment of media privacy standards;
- adequacy of the regulatory model; and

- lack of strong enforcement mechanisms in some media sectors.[1]

42.2 The ALRC has identified an ongoing need for an exemption for acts and practices of media organisations in the course of journalism. It recommends a number of improvements to the application of this exemption, however, including a definition of 'journalism' and a requirement that privacy standards developed and published by media organisations are 'adequate'.

Retaining an exemption for journalistic acts and practices

42.3 Under s 7B(4) of the *Privacy Act*, acts and practices of 'media organisations' are exempt from the operation of the Act, provided the acts or practices are undertaken 'in the course of journalism' at a time when the organisation is publicly committed to observe standards that deal with privacy. This exemption aims to ensure an appropriate balance between the public interest in freedom of expression and the public interest in adequately safeguarding the handling of personal information.[2]

42.4 Exemptions or exceptions for journalistic materials or news activities are provided in the privacy laws of many other countries.[3] In Canada, for example, the personal information protection principles do not apply to personal information collected, used or disclosed by a private sector organisation for journalistic, artistic or literary purposes.[4] In the United Kingdom, except in relation to data security, the data protection principles do not apply to the processing of personal data for journalistic, artistic or literary purposes where:

> (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,
>
> (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

---

1 See, eg, M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13; N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149; N Waters, 'Commonwealth Wheels Turn Again—A Cautious Welcome' (1999) 5 *Privacy Law & Policy Reporter* 127, 128. A similar view was expressed in submissions to the OPC Review: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 196–197.

2 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 4, [112]. The right to freedom of expression is recognised in the *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19(2), (3).

3 See, eg, *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) ss 4(2)(c), 7(1)(c); *Data Protection Act 1998* (UK) s 32; *Privacy Act 1993* (NZ) s 2(1); *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

4 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) ss 4(2)(c), 7(1)(c).

> (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.[5]

42.5 International instruments relating to the privacy of personal information also include express or implied exemptions for journalistic acts and practices. The European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) states that Member States shall provide for exemptions or derogations from certain provisions of the EU Directive

> for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[6]

42.6 Although the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) issued by the Organisation for Economic Co-operation and Development[7] do not provide specifically for an exemption or exception relating to journalistic activities or freedom of expression, they recognise that there may be exceptions to the privacy principles, which should be 'limited to those which are necessary in a democratic society'.[8]

42.7 The right to freedom of expression is guaranteed under numerous international human rights instruments.[9] The International Covenant on Civil and Political Rights (ICCPR), for example, provides that:

> 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.[10]

---

5 *Data Protection Act 1998* (UK) s 32(1). Under the *Data Protection Act 1998* (UK), the seventh data protection principle provides that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data': *Data Protection Act 1998* (UK) sch 1, principle 7.

6 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 9. See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), Recitals 17, 37.

7 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

8 Ibid, Guideline 4; Memorandum, [47].

9 See, eg, *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*: *United Nations Universal Declaration of Human Rights*, GA Res 217A(III), UN Doc A/Res/810 (1948) art 19; *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19; *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), art 10.

10 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19.

42.8 In Australia, only Victoria and the ACT have enacted bills of rights. In the remaining Australian jurisdictions, there are no formal, legislative guarantees of protection for freedom of expression. Freedom of expression is nevertheless given some limited forms of protection in Australian law—most relevantly, through the High Court's finding that the *Australian Constitution* contains an implied freedom of political communication.[11]

42.9 The Office of the Privacy Commissioner (OPC), in its review of the private sector provisions of the *Privacy Act* (OPC Review), noted that it had received very few inquiries and complaints about media organisations.[12] Privacy-related investigations also comprise a low proportion of investigations conducted by bodies charged with regulation of the media. From July 1996 to June 2006, the Australian Broadcasting Authority (and subsequently the Australian Communications and Media Authority (ACMA)), conducted a total of 82 privacy-related investigations involving commercial television; 23 of which were found to involve breaches.[13]

Submissions and consultations

42.10 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC expressed the preliminary view that—provided suitable limitations were in place—the *Privacy Act* should retain an exemption for media organisations.[14] The ALRC suggested, however that, where the relevant elements could be established, acts and practices within the scope of this exemption should be subject to the proposed statutory cause of action for a serious invasion of privacy.[15]

42.11 The importance of retaining an exemption for acts and practices in the course of journalism was put forward strongly by media organisations and their representative bodies in submissions in response to the ALRC's Issues Paper, *Review of Privacy* (IP 31)[16] and DP 72.[17] The Right to Know Coalition,[18] for example, commented:

---

11 In a series of cases culminating in *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, the High Court has held that the *Australian Constitution* must be read as impliedly protecting political communication.

12 During the period between 21 December 2001 and 31 January 2005, 1% of all the National Privacy Principles (NPPs) complaints closed by the OPC on the basis that they were outside of its jurisdiction concerned the media exemption: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

13 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

14 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [38.65].

15 Ibid, [38.70]. The statutory cause of action for invasion of privacy is discussed in Ch 74.

16 Free TV Australia, *Submission PR 149*, 29 January 2007; SBS, *Submission PR 112*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007; Australian Press Council, *Submission PR 83*, 12 January 2007; Australian Press Council, *Submission PR 48*, 8 August 2006.

17 Australian Broadcasting Corporation, *Submission PR 571*, 18 February 2008; The Herald and Weekly Times Pty Ltd, *Submission PR 568*, 11 February 2008; Right to Know Coalition, *Submission PR 542*, 21 December 2007; Australian Press Council, *Submission PR 411*, 7 December 2007.

18 The Right to Know Coalition is comprised of News Limited, Fairfax Media, Free TV Australia, Australian Subscription Television & Radio Association (ASTRA), Commercial Radio Australia, SBS, ABC, Sky News, Australian Associated Press (AAP), APN News and Media, Media Entertainment and Arts Alliance (MEAA) and West Australian Newspapers.

> if citizens are to effectively participate in a democracy, form opinion freely and protect their rights and interests, they need access to information either directly, or via the media … the sheer quantity of information makes it impossible for the public to keep itself properly informed in such a sophisticated and complex environment; it relies on the media to act as a conduit and provide information, commentary and opinion.[19]

42.12 The OPC submitted that, given the important role of a free press in a liberal democracy, and in the absence of strong evidence of abuse, it is unnecessary to remove the exemption for media organisations. The OPC suggested, however, that the exemption should be referred to as the 'journalism exemption', rather than the ALRC's suggested 'media exemption', as the former better reflects the limited scope of the exemption.[20]

42.13 Some stakeholders submitted that the balance between privacy rights and freedom of expression should be addressed by selective exceptions to some of the privacy principles, rather than by an exemption.[21]

42.14 The Right to Know Coalition did not support the application of the statutory cause of action to acts and practices that fell within the exemption for media organisations.[22] The Arts Law Centre of Australia also advised that it was 'highly concerned that the ALRC has indicated that the media exemption is not to apply to the proposed statutory cause of action'.[23]

ALRC's view

42.15 Freedom of expression is a fundamental human right, as recognised by art 19 of the ICCPR, and an integral element of a democratic society. As the European Court of Human Rights has expressed it:

> Freedom of expression constitutes one of the essential freedoms of a democratic society and one of the basic conditions for its progress and for every individual's self-fulfilment … it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'.[24]

42.16 As noted above, although Australia is a signatory to the ICCPR, there has been no implementation of this commitment in domestic law at the federal level through constitutional change or by the enactment a statutory Bill or Charter of Rights. As also

---

19 Right to Know Coalition, *Submission PR 542*, 21 December 2007.
20 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
21 I Turnbull, *Submission PR 378*, 5 December 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007. See also Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979).
22 Right to Know Coalition, *Submission PR 542*, 21 December 2007.
23 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.
24 *Case of Plon (Societe) v France* [2004] ECHR 200, [42].

noted above, the High Court nevertheless has introduced a measure of formal legal protection for freedom of expression through a series of cases in which it found that free speech must be implied in the fabric of the Constitution,[25] at least to the extent that the proper functioning of a democratic society such as ours requires

> the ability of the people of the Commonwealth as a whole to communicate, among themselves, information and opinions about matters relevant to the exercise and discharge of governmental powers and functions on their behalf.[26]

42.17 In *Lange*, the High Court stated that the test for constitutionality of any legislation arguably infringing political communication contained two limbs:

> First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end the fulfillment of which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government and the procedure prescribed by s 128 for submitting a proposed amendment of the Constitution to the informed decision of the people.[27]

42.18 Ironically, many of the same media organisations now strongly campaigning against any regulation or restriction of freedom of expression also have been among the most fervent opponents editorially of introducing any formal Charter of Rights in Australia. They also are among the most passionate critics of the High Court's 'implied free speech' cases—which are said to exemplify 'judicial activism' and the exercise of lawmaking powers more properly the function of Parliament.[28]

42.19 Freedom of expression and the balancing of competing legitimate interests were at the heart of the ALRC's review of sedition laws. In *Fighting Words: A Review of Sedition Laws in Australia*,[29] the ALRC noted that, whatever the formal legal protection accorded freedom of expression, there is a strong cultural preference and respect for free speech:

> Australians place a very high premium on freedom of expression and on the importance of robust political debate and commentary. The free exchange of ideas—however unpopular or radical—is generally healthier for a society than the suppression and festering of such ideas.[30]

---

25 Beginning with *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

26 *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1, [72].

27 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567.

28 See, for example, 'Sold a Bill of Rights', *The Australian* (Sydney), 22 December 2005, 11; P Kelly, 'Freedom Fighters to Face Great Divide', *The Australian* (Sydney), 11 April 2001, 13; 'Rights and Wrongs', *Sydney Morning Herald* (Sydney), 11 January 2001, 12.

29 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Ch 7.

30 Ibid, 10.

42.20 The principle of freedom of expression is not, however, absolute. All legal systems impose restrictions on certain forms of expression—for instance, where speech is defamatory or obscene, or is intended to incite the commission of a crime. The Privy Council, hearing an appeal from the High Court of Australia in 1936, observed:

> Free speech does not mean free speech; it means speech hedged in by all the laws against defamation, blasphemy, sedition and so forth; it means freedom governed by law … [31]

42.21 In deference to the critical importance of freedom of expression—particularly freedom of political communication—in our democratic system of government, the ALRC supports retaining an exemption in the *Privacy Act* for journalistic acts and practices. The ALRC also agrees with the OPC that, in order to reflect better the limited nature of this exemption, it should be referred to as the 'journalism exemption'.

42.22 Equally, there is a need to strike an appropriate balance between the public interest in maintaining freedom of expression and the public interest in adequately safeguarding the handling of personal information.[32] In the following sections of this chapter, the ALRC recommends two new limitations to the exemption for acts and practices in the course of journalism, namely that: a definition of 'journalism' should be introduced for the purposes of the *Privacy Act*; and media organisations must be committed to 'adequate privacy standards'.

42.23 Unfortunately, the self-regulatory mechanisms utilised by the media do not provide the entire answer to the balancing exercise. Unlike the position with, for example, doctors or lawyers, working journalists are not subject to any:

- formal educational requirements (basic or continuing) in order to qualify to practise;
- accreditation or registration procedures;
- binding code of ethics or professional standards (unless they are members of the relevant trade union—the Media, Entertainment and Arts Alliance (MEAA)—which is not a requirement to practice); or
- independent disciplinary authority with the power to investigate and impose meaningful sanctions (such as suspension or deregistration) for a serious breach of professional standards.

42.24 As discussed below, media organisations are subject to a range of voluntary industry standards (for example, those developed by the Australian Press Council (APC) for the print media) and regulations made under law (such as those promulgated

---

31 *James v Commonwealth* (1936) 55 CLR 1, 56.

32 See also, Ch 74.

by ACMA in respect of the broadcast media). Such sanctions for breach as exist provide few, if any, real remedies for individuals whose privacy rights have been seriously affected. With the exception of the broadcast media, nor, arguably, do they provide significant disincentives for further breaches.

42.25 Acts and practices in the course of journalism should remain subject to the recommended statutory cause of action. This is a separate question to an exemption from interferences with privacy under the *Privacy Act*. The statutory cause of action is discussed in Chapter 74.

Scope of the journalism exemption

42.26 In the course of this Inquiry, a number of stakeholders have expressed concerns about the scope of the journalism exemption.[33] In particular, stakeholders have suggested that the lack of definition of the term 'journalism', together with the wide definition of the term 'media organisation', 'effectively allows anyone to claim the exemption by setting up a "publishing enterprise"'.[34] This raises the question of whether any of the components of the exemption should be defined more comprehensively.

'Journalism'

42.27 The phrase 'in the course of journalism' is not defined in the *Privacy Act*, nor has it been judicially considered in Australia. Originally, the word 'journalism' was defined in the Privacy Amendment (Private Sector) Bill 2000 (Cth) as 'the collection, preparation and dissemination of news, current affairs, documentaries and other information to the public', including commentary and opinion on, or analysis of, this kind of material.[35] After the release of the report on the Bill by the House of Representatives Standing Committee on Legal and Constitutional Affairs,[36] the Australian Government amended the Bill to omit the definition of 'journalism'.[37]

---

33 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; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

34 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. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 195–199; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 72–74.

35 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13.

36 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000).

37 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [2]–[4].

42.28 One commentator has argued that

> the everyday meaning of 'journalism' would appear to include entertainment, infotainment and educational output of the media. Arguably, important issues of freedom of speech and the public interest role of the media are confined to news and current affairs.[38]

42.29 The OPC Review recommended in 2005 that the term 'in the course of journalism' be defined and that the term 'media organisation' be clarified in order to ensure that the exemption focuses on news and current affairs.[39] The Australian Government disagreed with this recommendation.[40]

Submissions and consultations

42.30 In DP 72, the ALRC proposed that 'journalism' should be defined in the *Privacy Act*. The ALRC expressed the preliminary view that an appropriate definition would be:

> the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public: (a) material having the character of news, current affairs or a documentary; or (b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary.[41]

42.31 This modified the definition of 'journalism' that was originally included in the Privacy Amendment (Private Sector) Bill by excluding the word 'information' from that definition.

42.32 The majority of stakeholders that commented on this issue supported the proposal to define 'journalism' for the purposes of the media exemption.[42] The Cyberspace Law and Policy Centre, for example, commented that:

> The proposed definition of 'journalism' achieves the objective of limiting the scope of the media exemption to those activities where there is a genuine competing public interest to be balanced against privacy.[43]

---

38 C Vietri, 'The Media Exemption under Information Privacy Legislation: In the Public Interest?' (2003) 8 *Media and Arts Law Review* 191.

39 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 198, recs 58, 59.

40 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 11.

41 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 38–1.

42 The Herald and Weekly Times Pty Ltd, *Submission PR 568*, 11 February 2008; 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; National Legal Aid, *Submission PR 521*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

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

42.33 The Department of Broadband Communications and the Digital Economy commented that the ALRC's proposal was consistent with the approach to regulation of broadcasting services.[44]

42.34 The OPC generally agreed that the *Privacy Act* should be amended to define 'journalism', and supported the ALRC's proposal to include news, current affairs and documentaries in such definition. The OPC suggested, however, that the ALRC should give further consideration to the approach taken in art 9 of the EU Directive—that is, that there should be an exemption to the *Privacy Act* where the processing of personal information is 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.[45]

42.35 A number of stakeholders questioned whether the proposed definition would exclude emerging mediums for conducting journalism, such as blogs.[46] The Australian Library and Information Association, for example, commented that the concept of 'the media' is changing rapidly, and suggested that protection might need to be widened to encompass this broad range of mediums.[47] The Right to Know Coalition submitted:

> What is regarded as journalism should not be determined *solely* by reference to the mechanism that is used to deliver it to the public. Regard should be had to the specific nature of what is being reported.[48]

42.36 Some stakeholders also questioned the appropriateness of limiting the subject matter that would be exempted from the *Privacy Act*. The Australian Subscription Television and Radio Association (ASTRA), for example, submitted that 'the proposal essentially declares what is important enough to be exempted, rather than letting the circumstances dictate when something is in the course of journalism, and when it is not'.[49] The APC noted that journalism

> is something more than just the straight reporting of, and commentary on, matters of economics, politics and social developments. Sports, travel, food and leisure, film, music and books, and popular culture are all as worthy of coverage, in the public interest.[50]

42.37 The Right to Know Coalition also questioned whether advertisements could be excluded from the definition of journalism. It noted that this approach could result in material presented in a news or current affairs story falling within the journalism

---

44 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

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

46 Australian Broadcasting Corporation, *Submission PR 571*, 18 February 2008; Right to Know Coalition, *Submission PR 542*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australian Library and Information Association, *Submission PR 446*, 10 December 2007; Australian Press Council, *Submission PR 411*, 7 December 2007.

47 Australian Library and Information Association, *Submission PR 446*, 10 December 2007.

48 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

49 ASTRA, *Submission PR 426*, 7 December 2007.

50 Australian Press Council, *Submission PR 411*, 7 December 2007.

exemption, but the exemption not applying where the same material is presented in an advertisement for the story.[51] Telstra commented that the *Privacy Act* is not the appropriate place for redefining journalism and that it cannot be considered in isolation from, for example, defamation law.[52]

42.38 More broadly, the Right to Know Coalition expressed concerns that the media is being caught up in proposals that are intended to address problems with internet material and websites of individuals and non-mainstream media organisations. It suggested that these problems are unrelated to media organisations that commit to complaint mechanisms. It submitted that 'any reforms designed to address problems occurring in this space must be tailored specifically to avoid impact on the activities of the members of the coalition'.[53]

ALRC's view

42.39 Including a definition of journalism in the *Privacy Act* will limit the scope of the exemption to acts and practices that are associated with a clear public interest in freedom of expression. In particular, there is a public interest in disseminating material with the character of news, current affairs and documentaries, and commentaries on these materials. By its very nature, this type of journalism informs, criticises and initiates debate on societal issues of public importance.[54]

42.40 The ALRC acknowledges, however, the potential for information other than 'news, current affairs and documentaries', and commentaries on these materials, to contribute to debates of general interest. The ALRC, therefore, recommends an additional limb to the definition of journalism for information where there is a recognisable public interest in disclosure. The appropriate public interest test in this context should be the same as the recommended public interest test for research—that is, where the public interest in disclosure outweighs the public interest in maintaining the level of privacy protection afforded by the model Unified Privacy Principles (UPPs).[55]

42.41 A key component of the ALRC's recommended definition of 'journalism' is its focus on the *character* of the relevant publication. This means that—provided the underlying nature of the material satisfies one of the limbs of the recommended definition—the manner in which the information is disseminated (for example, whether the information is portrayed satirically) is irrelevant. Similarly, provided the underlying character of the information did not change, the exemption would remain applicable if

---

51 Right to Know Coalition, *Submission PR 542*, 21 December 2007.
52 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
53 Right to Know Coalition, *Submission PR 542*, 21 December 2007.
54 See the decision of the Supreme Court of Sweden in *Case B 293–00*, discussed in L Bygrave, 'Balancing Data Protection and Freedom of Expression in the Context of Website Publishing—Recent Swedish Case Law' (2001) 8 *Privacy Law & Policy Reporter* 83.
55 See Ch 65.

the material was disseminated through a different medium; for example, in a blog or in the course of an advertisement.

'Media organisation'

42.42 The exemption for acts and practices in the course of journalism applies only to 'media organisations'. In the *Privacy Act*, a 'media organisation' is defined as an organisation (which includes an individual)[56] that collects, prepares or disseminates to the public, news, current affairs, information or documentaries; or commentaries and opinions on, or analyses of, such material.[57]

42.43 In DP 72, the ALRC recognised that the public interest in the media exemption applies beyond established media businesses and professional journalists, and proposed that the definition of 'media organisation' should remain as it currently stands.

42.44 The Right to Know Coalition supported retaining the definition of 'media organisation' in its current form, commenting that the current definition has a proper degree of flexibility to encompass emerging and future activities that properly fall under the umbrella of 'media'. It submitted:

> the definition appropriately recognises that media activities may be undertaken by an array of people or organisations who are exercising significant rights of freedom of communication and speech.[58]

42.45 The APC commented that the proposed definition of journalism was circular with the definition of 'media organisation' included in the *Privacy Act*. It was concerned that this could limit unnecessarily the operation of the exemption.[59]

42.46 The Australian Broadcasting Corporation (ABC) advised that the exemption under s 7B(4) in relation to acts and practices of 'media organisations' may not apply to the national broadcasters, as its programming materials do not relate to 'commercial activities'. If the exemption for agencies pursuant to s 7(1)(c) of the *Privacy Act* were to be removed,[60] the programming activities of the national broadcasters would be subject to the privacy principles. The ABC also suggested that the definition of 'media organisation' in the Act should be extended to include other media publication categories. [61]

---

56 An 'organisation' is defined, with certain exceptions, to mean an individual, a body corporate, a partnership, any other unincorporated association or a trust: *Privacy Act 1988* (Cth) s 6C.

57 Ibid s 6(1).

58 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

59 Australian Press Council, *Submission PR 411*, 7 December 2007.

60 See Rec 36–4.

61 Australian Broadcasting Corporation, *Submission PR 571*, 18 February 2008.

ALRC's view

42.47 The capacity for the journalism exemption to apply to organisations outside the mainstream news media is an important component of freedom of expression. As stated by the Supreme Court of the United States in *Associated Press v United States*:

> [Freedom of the press] rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society … Freedom to publish means freedom for all and not some.[62]

42.48 The journalism exemption should not be limited to established media businesses or professional journalists. Adequate limitations are provided through the other requirements for the exemption; in particular, the recommended definition of journalism[63] and the requirement for the organisation to be publicly committed to media privacy standards.[64]

42.49 In accordance with the ALRC's broader policy objective of achieving greater consistency, simplicity and clarity in the *Privacy Act*, the media exemption should apply equally to the national broadcasters and organisations that are engaging in journalism. This can be achieved by amending the definition of 'media organisation' to include an agency that has been specified in the regulations. At a minimum, this should include the ABC and the Special Broadcasting Service (SBS).

42.50 The ALRC also agrees that there is unnecessary circularity between the recommended definition of 'journalism' and the definition of 'media organisation'. This can be simplified by abridging the definition to 'an organisation whose activities consist of or include journalism'. This ensures that, as media publication categories evolve, agencies or organisations that engage in these activities remain covered (where appropriate) by the journalism exemption.

'News, current affairs and documentaries'

42.51 The definition of 'media organisation' and the recommended definition of 'journalism' centre on the dissemination of 'news', 'current affairs' and 'documentaries'. These terms are not defined in the *Privacy Act*. Definitions have been provided, however, in other Commonwealth legislation and legislative instruments. The *Broadcasting Services Act 1992* (Cth), for example, defines 'news or current affairs program' as meaning:

> (a) a news bulletin;
>
> (b) a sports news bulletin;

62 *Associated Press v US* (1945) 326 U.S. 1, [20].
63 Rec 42–1.
64 Rec 42–3.

> (c) a program (whether presenter-based or not) whose sole or dominant purpose is to provide analysis, commentary or discussion principally designed to inform the general community about social, economic or political issues of current relevance to the general community.[65]

42.52 A 'documentary program' is defined in the *Broadcasting Services (Australian Content) Standard 2005* (Cth) as 'a program that is a creative treatment of actuality other than a news, current affairs, sports coverage, magazine, infotainment or light entertainment program'.

42.53 In DP 72, the ALRC proposed that the terms 'news', 'current affairs' and 'documentary' should continue to be interpreted through their ordinary meaning. Only two stakeholders specifically commented on this issue. The Right to Know Coalition supported the ALRC's view that the terms 'news', 'current affairs' and 'documentary' should be interpreted according to their ordinary meanings and not defined in the *Privacy Act*. It noted that 'it is very unlikely that statutory definitions could appropriately capture the ambit of these terms. This would have the undesirable effect of excluding content that is otherwise appropriately included which would undermine the application of the media exemption'.[66] The ABC also supported leaving these words undefined.[67]

42.54 Given the wide import of the terms 'news', 'current affairs' and 'documentary', defining these terms in the *Privacy Act* would be impracticable. Instead, these terms should continue to be accorded their plain English meaning.

Recommendation 42–1 The *Privacy Act* should be amended to define 'journalism' to mean the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

(a) material having the character of news, current affairs or a documentary;

(b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary; or

(c) material in respect of which the public interest in disclosure outweighs the public interest in maintaining the level of privacy protection afforded by the model Unified Privacy Principles.

---

65 *Broadcasting Services Act 1992* (Cth) sch 6 cl 2(1).
66 Right to Know Coalition, *Submission PR 542*, 21 December 2007.
67 Australian Broadcasting Corporation, *Submission PR 571*, 18 February 2008.

Recommendation 42–2 The definition of 'media organisation' in the *Privacy Act* should be:

(a) amended to 'an organisation whose activities consist of or include journalism'; and

(b) expanded to include an agency that has been specified in the regulations. The regulations should specify, at a minimum, the Australian Broadcasting Corporation and the Special Broadcasting Service.

Media privacy standards

42.55 For a media organisation to fall within the journalism exemption, it must be

> publicly committed to observe standards that:
>
> (i) deal with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters); and
>
> (ii) have been published in writing by the organisation or a person or body representing a class of media organisations.[68]

42.56 The Revised Explanatory Memorandum for the private sector provisions of the *Privacy Act* notes that this exemption 'seeks to balance the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media'.[69] One way a media organisation might demonstrate its public commitment to standards dealing with privacy is to show that it is a member of a media industry body and that membership of that body requires it to subscribe to a code of conduct developed and published by the industry body.[70]

Current framework for media privacy standards

42.57 The majority of media organisations seek to satisfy the requirement of being publicly committed to observe standards that deal with privacy in the following manner:

- radio and television industry groups develop codes of practice in accordance with the *Broadcasting Services Act*;
- national broadcasters (the ABC and the SBS) develop codes of practice in accordance with their establishing legislation;

---

68 *Privacy Act 1988* (Cth) s 7(B)(4).
69 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 86.
70 Ibid, 85–86.

- print or online media organisations that are members of the APC are bound by its *Privacy Standards*; and

- journalists that are members of MEAA are bound by its *Code of Ethics*.

Broadcasting industry groups

42.58 Under the *Broadcasting Services Act*, each section of the broadcasting industry, in consultation with ACMA, must develop codes of practice.[71] Industry codes that have been approved by ACMA are included on ACMA's Register of Codes of Practice.

42.59 There is presently no specific requirement for ACMA to consider privacy issues before registering an industry code. Under s 130M of the *Broadcasting Services Act*, however, ACMA must be satisfied that, to the extent to which the code deals with one or more matters of substantial relevance to the community, it provides appropriate community safeguards for that matter or those matters.

42.60 Privacy provisions are included in the codes of practice developed for the following industry sectors: commercial television; commercial radio; subscription broadcast television; subscription narrowcast television; community television; community radio; and open narrowcast radio.[72]

42.61 These codes differ, however, in relation to the substance of the included privacy provisions. Some, but not all, of the codes of practice provide that certain programs must not use material relating to a person's personal or private affairs, or which invades a person's privacy, unless there is a public interest for the materials to be broadcast.[73] Some of the codes of practice provide that licensees should not broadcast the words of an identifiable person unless the person has been informed in advance or his or her consent was obtained before the broadcast.[74] Only two of the codes of practice address specifically the privacy interests of children.[75]

---

71 *Broadcasting Services Act 1992* (Cth) s 123.

72 *Commercial Television Industry Code of Practice* (2004); Commercial Radio Australia, *Codes of Practice & Guidelines* (2004); Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Broadcast Television* (2007); Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Narrowcast Television* (2007); Community Broadcasting Association of Australia, *Community Television Code of Practice*; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002); Australian Narrowcast Radio Association, *Codes of Practice Open Narrowcast Radio* (2007). There are no specific privacy provisions in the codes of practice developed for the open narrowcast television and radio sectors.

73 *Commercial Television Industry Code of Practice* (2004), s 4; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 2; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Broadcast Television* (2007), Code 3; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3.

74 *Commercial Television Industry Code of Practice* (2004), Code 4.3; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 6; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3.5; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Narrowcast Radio* (2007) Code 1.5; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002), Code 2.5; Australian

42.62 All of the codes of practice for the broadcast media cover the handling of complaints from the public.[76] Complaints about lack of compliance with a broadcasting code of practice can be made to ACMA where a written complaint has been made to the particular station, and: the station does not answer the complaint within 60 days; or the complainant is dissatisfied with the station's response.[77] ACMA must investigate such a complaint unless it is satisfied that the complaint is frivolous, vexatious or irrelevant.[78]

42.63 Where ACMA determines that a private sector broadcasting service has breached, or is breaching, a relevant code of practice, it may issue a notice directing a person to take remedial action to ensure compliance.[79] A failure to comply with such a notice is an offence under the *Broadcasting Services Act* and attracts a penalty.[80] In relation to commercial broadcasting, community broadcasting and subscription television services, a breach of a licensing condition also could lead to suspension or cancellation of the broadcasting licence.[81]

42.64 In 2007, for example, ACMA found that the Southern Cross Television breached the *Commercial Television Industry Code of Practice* by broadcasting material that invaded the privacy of a mother and her 12 year old child. In response to the breach findings, the licensee undertook to discuss the issues raised by ACMA's investigation with the relevant staff and to include the investigation in future staff training sessions.[82]

42.65 ACMA has been given new powers under the *Communications Legislation Amendment (Enforcement Powers) Act 2006* (Cth) to accept enforceable undertakings in relation to compliance with the *Broadcasting Services Act* and registered codes of practice. If ACMA considers that a person has breached such an undertaking, it may

---

Narrowcast Radio Association, *Codes of Practice Open Narrowcast Radio* (2007), Code 1.5. The *SBS Codes of Practice* also contains a similar provision: Special Broadcasting Service, *Special Broadcasting Service, SBS Codes of Practice (2006)*, Code 1.8.

75 *Commercial Television Industry Code of Practice* (2004), Code 4.3; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3.5.

76 *Commercial Television Industry Code of Practice* (2004), s 7; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 5; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Broadcast Television* (2007), Code 2; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Narrowcast Television* (2007), Code 2; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 2; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002), Code 7; Australian Narrowcast Radio Association, *Codes of Practice Open Narrowcast Radio* (2007), Code 2.

77 *Broadcasting Services Act 1992* (Cth) ss 148, 150.

78 Ibid ss 149, 151.

79 Ibid s 141(6).

80 Ibid s 142.

81 Ibid s 143.

82 Australian Communications and Media Authority, *Investigation Report No 1813*, 2007/884 (2007). This investigation arose out of a segment of *Today Tonight* reporting on an alleged mismanagement by the Child Support Agency in relation to the paternity testing of the complainant's child. The broadcast named the complainant and commented on her sexual past and financial status.

apply to the Federal Court of Australia for an order directing compliance with the undertaking, the payment of compensation for another person's loss or damage suffered as a result of the breach, or the payment to ACMA of the amount of any financial benefit the person has obtained that is reasonably attributable to the breach.

42.66 ACMA has developed *Privacy Guidelines for Broadcasters*, which provide an overview of the way in which ACMA will assess complaints concerning alleged breaches of the privacy provisions.[83] The Guidelines advise that, in considering complaints about intrusions into privacy, ACMA will consider two main questions: did the material relate to a person's private affairs; and was its broadcast warranted in the public interest.[84] Examples of public interest matters that may justify an intrusion into an individual's privacy include: criminal matters; public health or safety; consumer affairs or protection; matters of politics, government and public administration; matters relating to the conduct of organisations which impact on the public; and seriously anti-social conduct which causes harm to others.[85]

National broadcasters

42.67 The ABC is a statutory corporation and Australia's only national, non-commercial broadcaster. Its functions include to: provide within Australia broadcasting services of a high standard; transmit broadcasting programs to countries outside Australia; and encourage and promote the musical, dramatic and other performing arts in Australia.[86] The SBS is Australia's multicultural and multilingual public broadcaster. It was established under the *Special Broadcasting Services Act 1991* (Cth) to provide multilingual and multicultural radio and television services.[87]

42.68 The regulatory regime set out in the *Broadcasting Services Act 1992* (Cth) for national broadcasting services differs from that for other types of broadcasting services. The ABC and SBS develop their codes of practice through separate consultative processes and are required to inform ACMA about them.[88]

42.69 Privacy provisions are included in the codes of practice for both the ABC and SBS. The *ABC Code of Practice*, for example, provides that:

> The rights to privacy of individuals should be respected in all ABC content. However, in order to provide information which relates to a person's performance of public

---

83 Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), 1.

84 Ibid, 2.

85 Ibid, 4.

86 *Australian Broadcasting Corporation Act 1983* (Cth) s 6.

87 *Special Broadcasting Service Act 1991* (Cth) s 6. The ABC and SBS are covered by the *Privacy Act* except in relation to their program materials and datacasting content. The specific exemption that applies to the ABC and SBS is discussed further in the context of the public sector in Chapter 36. The ALRC is recommending that the national broadcasters should be included within the definition of 'media organisation'. The journalism exemption therefore would apply to the national broadcasters in the same way as it applies to industry media organisations.

88 *Broadcasting Services Act 1992* (Cth) pt 11 div 2; *Australian Broadcasting Corporation Act 1983* (Cth) s 8(1)(e); *Special Broadcasting Service Act 1991* (Cth) s 10(1)(j).

> duties or about other matters of public interest, intrusions upon privacy may, in some circumstances, be justified.[89]

42.70 The *SBS Code of Practice* contains a similar provision.[90] In addition, under the *SBS Code of Practice*, SBS is not to transmit the words of an identifiable person except in certain specified circumstances.[91]

42.71 Both the ABC and the SBS have in place internal complaint-handling processes.[92] If a member of the public is not satisfied with the handling of a complaint by a national broadcaster, he or she can have the complaint reviewed by ACMA.[93] If a complaint is upheld in relation to a national broadcaster, ACMA may recommend, by written notice, that the national broadcaster take action to comply with the relevant code of practice, or take other action as specified in the notice. Such action may include broadcasting or otherwise publishing an apology or retraction.[94] If the recommendation is not followed within 30 days, ACMA may give the responsible minister a written report on the matter, and the minister must table the report in Parliament.[95]

Print or online media organisations

42.72 The APC is a self-regulatory body that deals with the print media. Its stated objectives are to help preserve the freedom of the press within Australia and ensure that the press acts responsibly and ethically.[96]

42.73 The APC has published a set of *Privacy Standards* for the purposes of the media exemption under the *Privacy Act*.[97] The *Privacy Standards* deal with the collection, use and disclosure, quality and security of personal information; anonymity of sources; correction, fairness and balance; and the handling of sensitive information.

42.74 The APC receives and deals with complaints about possible breaches of these Standards, but it will not hear a complaint that is subject to legal action or possible legal action, unless the complainant is willing to sign a waiver of the right to such action. The APC secretariat will try to negotiate the settlement of a complaint, failing which a formal response will be sought from the publisher and sent to the complainant. If the complainant is not satisfied with the response, he or she, with the agreement of the newspaper, can seek a conciliation hearing conducted by the APC, or can immediately refer the matter to the APC for adjudication. If asked to adjudicate, the

---

89 Australian Broadcasting Corporation, *ABC Code of Practice* (2007), [2.8].
90 Special Broadcasting Service, *SBS Codes of Practice* (2006), [1.9].
91 Ibid, [1.8].
92 Australian Broadcasting Corporation, *ABC Code of Practice* (2007), [7]; Special Broadcasting Service, *SBS Codes of Practice* (2006), [8].
93 *Broadcasting Services Act 1992* (Cth) pt 11 div 2.
94 Ibid s 152.
95 Ibid s 153.
96 Australian Press Council, *About the Council* <www.presscouncil.org.au/pcsite/apc.html> at 6 May 2008.
97 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 1 May 2008.

APC's Complaints Committee holds a hearing and makes a recommendation to the APC. The APC has no power to penalise or make an order against a publication; it can only distribute the Committee's findings to the media and publish them in the APC's newsletters and annual reports.[98]

42.75 The APC is widening its remit to include online news sites that are willing to abide by its principles and privacy standards.[99] The APC anticipates that its *Privacy Standards* will apply to media organisations that publish on the internet in the same way as they apply to media organisations that publish in print.[100] The APC also is considering adopting a website Code of Conduct that would govern blog-related matters, both for contributors and those responsible for news media websites.[101]

Journalists

42.76 MEAA is the union and professional organisation for the media, entertainment, sports and arts industries.[102] Journalist members of the MEAA are bound by its *Code of Ethics*, which provides for certain privacy standards, including the requirement that journalists: do not place unnecessary emphasis on personal characteristics such as race, ethnicity and religious beliefs; identify themselves and their employer before obtaining an interview; and respect private grief and personal privacy.[103]

42.77 Where a person believes that a journalist member of the MEAA has breached the Code, he or she may make a formal complaint to the MEAA. If the MEAA finds the complaint proven, it can censure or rebuke the journalist, fine the journalist up to $1,000 for each offence, or expel the journalist from membership of the MEAA. Information about complaints against journalists is published and distributed on an annual basis to journalist members of the MEAA.[104]

Other media organisations

42.78 The journalism exemption is not confined to entities that fall within the mainstream media—it is open to an organisation to develop and administer its own

---

98 Australian Press Council, *How to Make a Complaint: An Overview* <www.presscouncil.org.au/pcsite/complain.html> at 6 May 2008.

99 Australian Press Council, *State of the News Print Media in Australia: 2007 Supplement to the 2006 Report* (2007), 7.

100 Ibid, 31.

101 Ibid, 33.

102 Media Entertainment and Arts Alliance, *Alliance Online* <www.alliance.org.au> at 6 May 2008.

103 Media Entertainment and Arts Alliance, *Media Alliance Code of Ethics* <www.alliance.org.au/code-of-ethics.html> at 6 May 2008, [2], [8], [11].

104 Alliance Online, *Code of Ethics Breaches: How to Complain* <www.alliance.org.au/media/ethics_breach.htm> at 6 May 2008. This complaints process, however, is not frequently used. The Senate Select Committee on Information Technologies reported that, in 1995–96, the New South Wales Branch of the Australian Journalists Association—the section of MEAA dealing with journalism—received 37 formal complaints, of which 14 proceeded to a hearing by the Judiciary Committee. The 37 complaints included five matters relating to failure to respect private grief and personal privacy. Parliament of Australia—Senate Select Committee on Information Technologies, *In the Public Interest: Monitoring Australia's Media* (2000), 44.

media privacy standards. Presently, there are no requirements for, or guidance on, the criteria that should be included in these standards.

Options for reform

42.79 Concerns have been raised that the present provisions governing media privacy standards may be insufficient to guard against breaches of privacy—or to provide adequate enforcement mechanisms or remedies—if media organisations or journalists behaved irresponsibly.[105] The ALRC has identified a range of options for enhancing the operation of this requirement, which are considered further below. These include:

- requiring media privacy standards to deal with privacy in an adequate way;
- prescribing standards for the handling of certain categories of personal information—for example, the personal information of children and young people;
- requiring media privacy standards to include greater enforcement mechanisms and complaint-handling processes; and
- specifying that 'public commitment' to observe privacy standards includes the need for active conduct evidencing such commitment.

'Adequacy' of media privacy standards

42.80 The terms of the journalism exemption presently are silent on what should be included within the standards developed by media organisations dealing with privacy. Arguably, at least some of the current media privacy standards are lacking in scope and detail. The APC's *Privacy Standards*, for example, do not contain an equivalent of NPP 1.3 (ensuring that individuals about whom an organisation has collected personal information are aware of certain matters) or NPP 9 (the 'Transborder Data Flows' principle). They also may be more lax in several respects than some of the other NPPs.[106]

42.81 In the OPC Review, the OPC stated that:

> It is not clear if this section enables the Commissioner to decide whether or not the standard deals with privacy in an adequate way in the course of establishing whether or not a media organisation is publicly committed to a standard.[107]

---

105 See, eg, Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [4.47]–[4.48].

106 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 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), 198.

42.82 In DP 72, the ALRC proposed that media organisations seeking to rely upon the journalism exemption should be required to be publicly committed to observe standards that deal *adequately* with privacy in the context of the activities of a media organisation.[108] The ALRC further proposed that the OPC, in consultation with ACMA and peak media representative bodies, should develop and publish guidelines containing the criteria for assessing the adequacy of media privacy standards.[109]

42.83 The proposed scheme would work as follows: where the Privacy Commissioner receives a complaint about an act or practice of a media organisation in the course of journalism, he or she first would assess the adequacy of the privacy standards to which the media organisation was publicly committed. If these standards addressed the criteria included in the OPC's guidelines they would be determined to be 'adequate'. The Privacy Commissioner, therefore, would refer the complaint back to the body responsible for oversight of the standards. If the standards did not meet these criteria, however, the journalism exemption would not apply and the Privacy Commissioner would determine the complaint in accordance with the model UPPs.

42.84 Several other Commonwealth laws provide requirements that must be met in an 'adequate' manner, including for the: provision of child support;[110] review of administrative decisions;[111] and adoption of benefit fund rules for life insurance.[112] These laws vary, however, in the degree of legislative or other guidance provided on how adequacy should be met. The *Administrative Decisions (Judicial Review) Act 1977* (Cth), for example, allows courts to refuse applications for administrative review where adequate provision is made by another law for the applicant to seek a review. Adequacy in this context has been interpreted on its plain English meaning of 'sufficient' or 'suitable'.[113] In comparison, the *Life Insurance Act 1995* (Cth) provides that 'friendly societies' will have 'adequately adopted' benefit fund rules where they: have been adopted in a way set out in prudential rules or standards; and the Australian Prudential Regulatory Authority considers that adoption of the rules in this way adequately takes into account the interests of members.[114]

42.85 Under s 130M of the *Broadcasting Services Act*, ACMA must register an industry code if it is satisfied that the code meets a number of requirements, including that is provides 'appropriate community safeguards' for matters of substantial relevance to the community. ACMA also must be satisfied that, to the extent a code deals with matters that are not of substantial relevance to the community, the code deals with those matters in an appropriate way.[115]

---

108 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 38–4.
109 Ibid, Proposals 38–2, 38–3.
110 *Family Law Act 1975* (Cth) s 72.
111 *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 10(2)(b).
112 *Life Insurance Act 1995* (Cth), s 16B(1), (2).
113 *Edelsten v Minister for Health* (1994) 58 FCR 419.
114 *Life Insurance Act 1995* (Cth), s 16B(1), (2).
115 *Broadcasting Services Act 1992* (Cth) s 130M.

Submissions and consultations

42.86 The clear majority of stakeholders that commented on this issue—with the exception of most media organisations[116]—supported the proposals that the *Privacy Act* should be amended to provide that the standards must deal adequately with privacy in the context of the activities of a media organisation,[117] and that the OPC, in consultation with ACMA and other peak media representative bodies, should issue criteria to assess such adequacy.[118] The OPC, for example, noted that the inclusion of the term 'adequately' would clarify that the standards must be 'robust and of substance'. The OPC suggested that ACMA's *Privacy Guidelines for Broadcasters* could usefully inform these criteria.[119] The Department of Broadband, Communications and the Digital Economy advised that the proposed model was consistent with the co-regulatory approach to the regulation of the broadcast media.[120]

42.87 Media organisations, however, expressed a number of concerns about the potential application of this provision. The Right to Know Coalition submitted that the proposed role for the OPC in assessing the adequacy of privacy standards was 'unnecessary' as the ongoing review process of the various industry codes of practice contains mechanisms through which the OPC can provide input. In particular, it argued that the proposal would create 'regulatory uncertainty around the availability of the media exemption that is inappropriate'. In the Coalition's view, assessing whether the privacy standards of a particular media organisation are adequate necessarily will involve questions of interpretation and debate. Until such debate is resolved, media organisations are left with uncertainty as to the regulatory regime by which they are covered.[121]

42.88 The APC advised that, although there may be sound reasons for expecting that some media organisations should revise their privacy standards, it considers its *Privacy Standards for the Print Media* to be adequate. It agreed to consult with the OPC to address any changes that might be necessary.[122]

---

116 Notably, the Herald and Weekly Times supported the proposed changes to the requirements for media privacy standards.

117 The Herald and Weekly Times Pty Ltd, *Submission PR 568*, 11 February 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

118 The Herald and Weekly Times Pty Ltd, *Submission PR 568*, 11 February 2008; 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; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

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

120 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

121 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

122 Australian Press Council, *Submission PR 411*, 7 December 2007.

42.89 Some stakeholders suggested modifications to the proposed process for developing and issuing these guidelines. ACMA commented that the criteria for assessing the adequacy of media privacy standards should be developed jointly by ACMA and the OPC.[123] The OPC submitted that, in order to promote regulatory stability, the adequacy criteria should be set out in a legislative instrument made by the Privacy Commissioner and disallowable by Parliament.[124] Several stakeholders suggested that the OPC should publish the criteria as binding rules.[125]

Special categories of personal information

42.90 In the course of this Inquiry, stakeholders raised particular concerns about the manner in which the media handles certain types of personal information, including:

- the personal information of children and young people;
- personal health information; and
- personal information associated with judicial proceedings.

Individuals under the age of 18

42.91 The only set of Australian broadcasting standards or principles that deal specifically with the privacy of children is the *Commercial Television Industry Code of Practice*.[126] Section 4.3.5.1 states that

> licensees must exercise special care before using material relating to a child's personal or private affairs in the broadcast of a report of a sensitive matter concerning the child. The consent of a parent or guardian should be obtained before naming or visually identifying a child in a report on a criminal matter involving a child or a member of a child's immediate family, or a report which discloses sensitive information concerning the health and welfare of a child, unless there are exceptional circumstances or an identifiable public interest reason not to do so.

42.92 In consultations with the ALRC, some examples were given of cases where a breach of privacy of a young person had been found, but there were minimal consequences for the media organisations involved.[127] Overall, however, the ALRC received limited comments from stakeholders expressing concern about the treatment of children and young people in the media.[128] A number of young people consulted

---

123 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

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

125 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

126 Although the ACMA *Privacy Guidelines for Broadcasters* (2005) make reference to the *Commercial Television Industry Code of Practice* and reproduce in appendices relevant sections from that Code relating to children. For the purposes of the Code, a 'child' means a person under 16 years: s 4.3.5.2.

127 Youth Issues Roundtable, *Consultation*, Melbourne, 7 February 2007.

128 A number of comments were received in relation to the media treatment of children and young people accused of or charged with criminal offences. This issue is dealt with in Ch 69.

assumed that, because they sometimes see faces and identities blurred out, privacy protections are in place and working effectively.[129]

42.93 The New South Wales Commission for Children and Young People suggested that the existing media exemption from the *Privacy Act* does not protect adequately the privacy rights of children and young people, and that there should be a legislative requirement that broadcasters include, within their industry privacy standards, a standard that relates to children and young people specifically.[130] It considered that the standard should require broadcasters to consider the best interests of the child or young person, even where informed consent has been obtained from the child or his or her parent.

42.94 The best interests approach has been adopted in New Zealand. In 1999, in response to concerns over two particular cases,[131] the Broadcasting Standards Authority of New Zealand amended the privacy principles that are imposed on broadcasters to include an additional privacy principle relating especially to children.[132] The current principle reads:

> Children's vulnerability must be a prime concern to broadcasters, even when informed consent has been obtained. Where a broadcast breaches a child's privacy, broadcasters shall satisfy themselves that the broadcast is in the child's best interests, regardless of whether consent has been obtained.
>
> For the purpose of these Principles only, a 'child' is defined as someone under the age of 16 years. An individual aged 16 years or over can consent to broadcasts that would otherwise breach their privacy.[133]

42.95 In DP 72, the ALRC considered the possibility of requiring media organisations to obtain consent from a person with parental responsibility for the child or young person under a certain age before identifying or otherwise publishing personal information about the child or young person. The ALRC also considered whether additional obligations should be imposed on media organisations to consider the best interests of the child or young person, even where parental consent is obtained. Consistent with its broader approach to the journalism exemption, the ALRC did not suggest that particular obligations be placed on media organisations in relation to children and young people. It was proposed, however, that the OPC should include consideration of the privacy of children and young people in the proposed criteria for

---

129 Youth Consultation, *Consultation PC 228*, Sydney, 5 December 2007; Youth Consultation, *Consultation PC 225*, Sydney, 7 December 2007.

130 NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007.

131 Both cases involved broadcasting of a child and sensitive personal details with parental permission: see M des Tombe, '"Get that Camera Out of My Face!" A Look at Children, Privacy and the Broadcasting Standards' (2000) 31 *Victoria University of Wellington Law Review* 577; K Ridley, 'Children and the Broadcasting Media: Respect for the Integrity and Rights of the Child?' (2000) 15(May) *Social Work Now* 6.

132 T McBride, 'Recent New Zealand Case Law on Privacy: Part II—The Broadcasting Standards Authority, the Media and Employment' (2000) 6 *Privacy Law & Policy Reporter* 133, 137.

133 New Zealand Government Broadcasting Standards Authority, *Privacy Principles* (2006).

assessing the adequacy of media privacy standards for the purposes of the media exemption.[134]

42.96 All submissions that addressed this issue supported the proposal.[135] While giving support, the Law Society of New South Wales urged that the approach to assessing media privacy standards be more comprehensive than what was suggested in DP 72. The Law Society suggested that, to assess the adequacy of media privacy standards, the Privacy Commissioner should obtain wide advice, potentially through establishing an advisory panel.[136]

42.97 SBS raised more general concerns relating to the ALRC's proposals to set an age under which parental consent would be required before a young person could disclose personal information.[137] SBS was concerned that this would have the undesirable effect of excluding young people under that age from participating in interviews and public discussions.

> Where an individual under 18 volunteers information about themselves which could constitute private information, it is SBS's view that the journalist's assessment of whether that individual has the capacity to understand the implications of that decision should be paramount.[138]

Health information

42.98 The broadcasting of personal health information received widespread public attention in 2007 when Channel 7 allegedly used confidential medical records in a story about illegal drug use by Australian Football League (AFL) players. Channel 7 named the club of two players who had allegedly been referred for treatment for illicit drug use, but not the players themselves, before the Victorian Supreme Court issued an injunction preventing further broadcasting. After being boycotted by AFL players, Channel 7 issued an apology, agreed not to contest the injunction and not to publish or re-publish details from the news report.[139]

42.99 A similar incident occurred in 2006, when *The Age* newspaper and Nationwide News Pty Ltd received information about the identity of three AFL players who, it was said, had been the subject of positive tests under the AFL Illicit Drugs Policy. The

---

134 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 60–8.

135 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; 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.

136 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

137 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 60–1.

138 Special Broadcasting Service, *Submission PR 530*, 21 December 2007.

139 See, eg, 'Seven Apologises for AFL Drugs Story', *ABC News* (online), 4 September 2007, <www.abc.net.au/news>; K Bice and AAP, 'Court Extends Injunction on AFL Details', *The Australian* (online), 30 August 2007, <www.theaustralian.news.com.au>.

Australian Football League (AFL) successfully brought an action under breach of confidence for a permanent injunction to restrain the newspapers from publishing any material that would identify an AFL player that has tested positive to use of illicit drugs under the policy. [140]

42.100 The only set of Australian broadcasting standards or principles that deal specifically with the privacy of health information is the APC's *Privacy Standards*, which provide that:

> Media organisations should not place any gratuitous emphasis on the categories of sensitive personal information listed in Principle 7, except where it is relevant and in the public interest to report and express opinions in these areas.[141]

42.101 The AFL Players' Association submitted that the criteria issued by the OPC for assessing the adequacy of media privacy standards should 'include that the standards contain a prohibition against publication of an individual's personal medical information'.[142] This submission was supported by the Australian Professional Footballers' Association.[143] The Centre for Law and Genetics, in its submission on IP 31, suggested that the media exemption should be limited to the use of non-sensitive personal information.[144]

Personal information connected with legal proceedings

42.102 Open justice is a fundamental principle of the common law,[145] encompassing access by the media, and the right for the media to report on proceedings.[146] As noted in Chapter 35, however, some legislation recognises that certain proceedings may contain particularly sensitive information and should be subject to restricted media reporting. These include laws restricting the identification of: victims, and persons accused, of sexual assault;[147] parties to, and witnesses in, family law proceedings;[148] children involved in criminal proceedings;[149] and spent convictions.[150]

---

140 *Australian Football League v The Age Company Ltd* [2006] 15 VR 419. The AFL Illicit Drugs Policy was introduced on 14 February 2005. It applies to the use of illicit drugs—including stimulants, narcotics and cannabinoids—by players and to testing for such drugs out of competition. The primary focus of the policy is the education and rehabilitation of players: see *Australian Football League v The Age Company Ltd* [2006] 15 VR 419, [5].

141 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 1 May 2008, Principle 7. The categories of sensitive information referred to in this principle are race, religion, nationality, colour, country of origin, gender, sexual orientation, marital status, disability, illness or age of an individual or group. Australian Press Council, *Statement of Principles* <www.presscouncil.org.au/pcsite/complaints /sop.html> at 11 August 2006, Principle 7.

142 AFL Players' Association, *Submission PR 393*, 7 December 2007.

143 Australian Professional Footballers' Association, *Submission PR 430*, 10 December 2007.

144 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

145 See, eg, *John Fairfax & Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465.

146 See: *Regina v Denbigh Justices, Ex Parte Williams* [1974] QB 759, 765.

147 See, eg, *Crimes Act 1900* (NSW) s 578A; *Judicial Proceedings Act 1958* (Vic) s 4(1A), (1B); *Criminal Law (Sexual Offences) Act 1978* (Qld) ss 6, 7, 8; *Evidence Act 1906* (WA) s 36C; *Evidence Act 1929* (SA) s 71A; *Evidence Act 2001* (Tas) s 194K; *Evidence (Miscellaneous Provisions) Act 1991* (ACT); *Sexual Offences (Evidence and Procedure) Act 1983* (NT) ss 6, 7.

42.103 At present, the only Australian broadcasting standards or principles that deal specifically with reporting personal information connected to legal proceedings is the APC's *Privacy Standards*, which provide:

> Unless otherwise restricted by law or court order, open court hearings are matters of public record and can be reported by the press. Such reports need to be fair and balanced. They should not identify relatives or friends of people accused or convicted of crime unless the reference to them is necessary for the full, fair and accurate reporting of the crime or subsequent legal proceedings.[151]

42.104 In submissions to this Inquiry, stakeholders expressed concerns about the reporting of personal information in the context of legal proceedings.[152] Dr Ian Turnbull commented, for example, that although the open court system is an important aspect of Australia's justice system, 'excessive media attention where an accused has been acquitted can in many cases be a punishment in its own right or an unjust punishment to those who just happen to be caught up in circumstances'.[153]

42.105 National Legal Aid submitted that it had

> specific concerns about reporting details of people involved in legal matters where this involves a breach of law, court orders or is a consequence of a breach of privacy by a law enforcement agency or other body.[154]

42.106 National Legal Aid commented that some form of civil or administrative accountability would be preferable to the penal sanctions that apply to such actions.[155]

Enforcement mechanisms

42.107 Concerns have been raised about the processes for ensuring compliance with media privacy standards. The APC's *Privacy Standards*, for example, only can be enforced through the complaint process of the APC**,** which only has jurisdiction over members who have voluntarily accepted it.[156] In addition, it has been argued that the sanction imposed by the APC (publication of findings of non-compliance) is not a deterrent.[157] Similarly, the MEAA only has a limited range of remedies and no power to act against or sanction a non-member and there is no membership requirement or other form of certification or registration of journalists.

---

148 See, eg, *Family Law Act 1975* (Cth) s 121.

149 See, eg, *Children (Criminal Proceedings) Act 1987* (NSW) s 11; *Crimes (Family Violence) Act 1987* (Vic) s 24; *Juvenile Justice Act 1992* (Qld) ss 234, 301; *Young Offenders Act 1993* (SA); *Youth Justice Act 2007* (NT) ss 43, 50.

150 See, for example: *Crimes Act 1914* (Cth) Part VIIC; *Criminal Records Act 1991* (NSW); *Criminal Law (Rehabilitation of Offenders) Act 1986* (Qld); *Criminal Records (Spent Convictions) Act* (NT).

151 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 1 May 2008, Principle 7.

152 See National Legal Aid, *Submission PR 521,* 21 December 2007; I Turnbull, *Submission PR 378,* 5 December 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

153 I Turnbull, *Submission PR 378,* 5 December 2007.

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

155 Ibid.

156 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149.

157 Ibid.

42.108 In response to some submissions on IP 31 that raised concerns about mechanisms for enforcing media privacy standards,[158] the ALRC suggested that enforcement powers and sanctions for non-compliance with media privacy codes could be addressed by including the adequacy of these powers and sanctions as a consideration for the 'adequacy' of these standards.[159]

42.109 PIAC supported including requirements for 'effective enforcement powers and sanctions' in the criteria for assessing the adequacy of media privacy standards.[160] The Cyberspace Law and Policy Centre submitted that the standards should include a requirement to submit to an external dispute resolution scheme.[161]

42.110 The APC, however, was 'strongly of the view that no government body, whether the OPC or any other, should have the power to oversight the Council's handling of complaints'. It submitted that 'such review would be contrary to the principle that the press should be independent, and free from government control or intervention'. The APC advised, in relation to its own processes, that:

> The Council's sole punitive power, that of the adjudication printed by the cited publication, is more than adequate. … The ALRC might note the comments of one metropolitan newspaper editor who stated that he would rather pay a fine of $25,000 than have to publish a critical adverse adjudication, issued by his peers telling him that he had breached the ethical principles of journalism. The Council is aware from discussions with them that editors are significantly displeased when they have to place adverse adjudications in the valuable editorial space of their publications and that this possibility gives rise to a greater awareness of the privacy issues involved during the editorial decisionmaking processes on questionable stories.[162]

'Public commitment' to media privacy standards

42.111 For a media organisation to fall within the journalism exemption, it must be 'publicly committed' to observe media privacy standards. Some stakeholders have raised concerns that the notion of 'public commitment' is unclear[163] and that the requirement can be satisfied without any independent assessment.[164]

42.112 In DP 72, the ALRC proposed that the OPC should clarify that, in order for the media exemption to apply, 'public commitment' by media organisations to observe privacy standards not only requires *express* commitment, but also *conduct* evidencing commitment to observe those standards.[165] A significant number of stakeholders

---

158 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007.

159 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [38.113].

160 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

162 Australian Press Council, *Submission PR 411*, 7 December 2007.

163 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

164 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.

165 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 38–5.

supported this proposal.[166] PIAC, for example, noted that 'express commitment to observe privacy standards is meaningless if a media organisation engages in conduct that ignores these standards'.[167] The OPC agreed that media organisations should bear the onus of proving that they have taken 'active and positive steps towards complying with published privacy standards'.[168]

42.113 ACMA submitted that, if the OPC issues guidance to clarify the meaning of the term 'publicly committed' in s 7B(4) of the *Privacy Act*, it should specify that the relevant codes registered under the *Broadcasting Services Act* meet this requirement. ACMA also submitted that further consideration should be given to what conduct might be required by a media organisation to evidence commitment to the privacy standards—for example, whether a media organisation should be required to provide regular training to staff on the requirements on the standards.[169]

42.114 The Right to Know Coalition did not support the proposal. It submitted that Australia already has in place a 'comprehensive media privacy framework' and that the media's commitment to its published privacy standards is evidenced by the consistently low number of complaints, investigations and breach findings. The Coalition submitted that OPC guidance in this area 'would risk imposing further regulatory burden on media in circumstances where there is no identifiable public interest reason for doing so'.[170]

ALRC's view

'Adequacy' of media privacy standards

42.115 In order to qualify for the journalism exemption, organisations should be publicly committed to standards that deal *adequately* with privacy in the context of the activities of a media organisation. This is an important mechanism to ensure that the standards being relied upon are robust and of substance—while respecting the need for a high degree of media autonomy in order to protect freedom of expression—which is vital for the Australian Parliament's stated objective of ensuring safeguards for the handling of personal information. A requirement for adequacy also provides the framework through which a range of issues associated with media organisations' handling of personal information, including categories of personal information that raise particular privacy concerns and compliance mechanisms, can be addressed.

---

166 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; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

167 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

169 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

170 Right to Know Coalition, *Submission PR 542*, 21 December 2007.

42.116 The ALRC recommends that the journalism exemption set out in s 7B(4) of the *Privacy Act* should incorporate the plain English meaning of 'adequate'. Based on the interpretation of the word 'adequate' in the context of administrative review, this would require media privacy standards to be 'sufficient' or 'suitable' for the particular media organisation at issue. For example—to meet the requirement of 'adequacy'—a media organisation that deals regularly with children and young people may need to include in its standards clear provisions about how the capacity of individuals under the age of 18 will be assessed. For media organisations that only rarely deal with children and young people, however, these provisions may not be necessary.

42.117 In order to promote regulatory certainty, however, clear guidance should be available to media organisations about how the requirement for adequacy will be assessed. The ALRC recommends that the OPC, in consultation with ACMA and other peak media representative bodies, should develop two tools to provide this guidance: guidelines for adequate media privacy standards; and a template privacy standard.

42.118 For the vast majority of media organisations, sufficient guidance can be provided by setting out criteria that should be addressed in their media privacy standards. Providing high-level principles, rather than prescriptively setting out what those standards should be, balances the need for regulatory certainty with the independence associated with the self-regulatory and co-regulatory frameworks. The ALRC agrees with the OPC's submission that these criteria usefully could be informed by ACMA's *Privacy Standards for the Broadcast Media*.

42.119 For media organisations that do not fall under the umbrella of ACMA, the APC or other established media representative bodies, however, translating high-level criteria into standards capable of practical application is potentially onerous. Therefore, the ALRC recommends that the OPC, in consultation with ACMA and peak media representative bodies, also should develop template media privacy standards. This template would be used as a tool to assist (in particular, small, independent) media organisations to meet the requirement of adequate media privacy standards. The ALRC is not recommending that adoption of the template be mandatory, but rather that it provide a model.

42.120 The ALRC does not recommend that privacy codes must be approved specifically by the Privacy Commissioner in order to benefit from the journalism exemption. The ALRC considers, however, that a mechanism could be put in place to ensure that codes registered by ACMA automatically meet the 'adequacy' requirement under the *Privacy Act*. In the context of telecommunications, the ALRC recommends that ACMA only should be able to register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act* if it has consulted with, and taken into consideration, any comments or suggested amendments of the Privacy Commissioner.[171] A similar process could be undertaken in the broadcasting sector—

171 Rec 71–18.

for example, as a component of ACMA's assessment of whether an industry code provides appropriate safeguards for matters of substantial relevance for the community.[172]

Special categories of personal information

42.121 Particular concerns have been raised in this Inquiry relating to the reporting of certain types of personal information by media organisations, including: personal information about children and young people; sensitive personal information, including health information; and personal information connected to legal proceedings.

42.122 The ALRC's recommendations to improve the adequacy of privacy standards that must be adhered to by media organisations provides an effective response to the concerns raised. Given its approach to the media exemption in general, the ALRC is not recommending particular standards that should be met by media organisations in relation to these types of information. The ALRC suggests, however, that, in developing the criteria for adequate media privacy standards and template privacy standards recommended above, the OPC and peak media representative bodies should consider:

- issues regarding parental consent when handling the personal information of children and young people; and consider the best interests of the child or young person even where parental consent is obtained;

- whether the personal information falls within the definition of 'sensitive information' for the purposes of the *Privacy Act*; and

- whether reporting the personal information could result in any unfair prejudice to victims, people accused or convicted of crime, or relatives or friends of such persons.

Enforcement mechanisms

42.123 Enforcement powers and sanctions are an important consideration to determine whether a particular media privacy standard is 'adequate' for the purposes of the journalism exemption. The ALRC does not consider monetary sanctions to be the only, or necessarily the most appropriate, enforcement mechanism. The ALRC acknowledges the APC's advice that the disincentive of peer disapproval may be just as relevant to the adequacy of enforcement mechanisms as monetary sanctions. Where a media organisation clearly can demonstrate that its enforcement mechanisms promote 'moral deliberation and reflection' in such a way that practitioners 'internalise the

172 *Broadcasting Services Act 1992* (Cth) ss 130M(1)(d).

moral norms espoused by the profession', this could be taken into account when assessing the adequacy of the enforcement mechanisms.[173]

'Publicly committed' to media privacy standards

42.124 For a media organisation to meet the requirement of being 'publicly committed' to media privacy standards, it must both expressly commit to observing the standards and evidence conduct of such observance. This requirement, however, is sufficiently clear in the present wording of the journalism exemption.

Recommendation 42–3 The *Privacy Act* should be amended to provide that media privacy standards must deal *adequately* with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters).

Recommendation 42–4 The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority and peak media representative bodies, should develop and publish:

(a) criteria for adequate media privacy standards; and

(b) a template for media privacy standards that may be adopted by media organisations.

Reassessing the framework for media regulation?

42.125 As noted above, Australia has in place a self-regulatory model for the print media and a co-regulatory model for the broadcast media. This framework also has been adopted in a number of overseas jurisdictions, including the United Kingdom[174] and New Zealand.[175] In light of changes to the media—in particular, technological convergence—this regulatory model no longer may be suitable.

---

173 I Freckleton, 'Enforcement of Ethics' in M Coady and S Bloch (eds), *Codes of Ethics and the Professions* (1996) 130.

174 In the United Kingdom, the print media are self-regulated and overseen by the Press Complaints Commission. The Press Complaints Commission is an industry body that deals with complaints from members of the public about the editorial content of newspapers and magazines. In relation to the broadcasting media, the Office of Communications was established under the *Office of Communications Act 2002* (UK) as the regulator for the United Kingdom communications industries. It applies a single Broadcasting Code across the broadcasting industry. The Office of Communications is charged with handling and adjudicating privacy complaints under s 326 of the *Communications Act 2003* (UK).

175 The print media in New Zealand is overseen by the New Zealand Press Council, a private body established in 1972 by newspaper publishers and journalists to provide an independent forum for the resolution of public complaints. The broadcast media are subject to higher regulatory standards, pursuant to a co-regulatory model under the *Broadcasting Act 1989* (NZ). The Act establishes the Broadcasting Standards Authority as a supervisory body whose functions include: receiving and determining

42.126 In 1997, the Senate Select Committee on Information Technologies was established to evaluate the appropriateness, effectiveness and privacy implications of the self-regulatory framework of the information and communications industries—including the print media, television, radio and telecommunications sectors.[176] The Senate Committee found that there were numerous instances that question the success of self-regulation and co-regulation by the information and communications industries. The Senate Committee recommended that an independent statutory body—the Media Complaints Commission—be established as a single reference point to deal with all complaints against Australia's information and communications industries.[177] Two other inquiries into the broadcasting media—by the Productivity Commission inquiry into broadcasting services in Australia and by the Australian Broadcasting Authority into commercial radio—also found flaws with the current regulatory models.

42.127 In the course of this Inquiry, a number of stakeholders made submissions relating to the framework for media regulation. Media organisations and their representative bodies submitted that the current regulatory model should remain.[178] It was suggested that the advantages of self-regulation are that: it is inexpensive and efficient;[179] and the newspaper and magazine publishing industry is committed to it and agrees to abide by the APC's rulings to publish adjudications where appropriate.[180] Media stakeholders submitted that a body appointed by the government to oversee the media is undesirable,[181] as it would interfere with the right to publish freely without fear of government intervention, which is fundamental to a democratic society.[182]

42.128 As noted above, however, the ALRC has ongoing concerns about the capacity of a self-regulatory system to preserve the tenuous balance between the public interest in freedom of expression and the public interest in adequately safeguarding the handling of personal information.

42.129 In Chapter 71, the ALRC recommends that the Australian Government should initiate a review to consider the ongoing effectiveness of the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth).

---

complaints; encouraging the development and observance by broadcasters of codes of practice in relation to individual privacy; approving codes; and developing and issuing codes itself where the Authority considers that it is appropriate to do so: *Broadcasting Act 1989* (NZ) ss 20, 21(a), (e)(viii), (f), (g).

176 Parliament of Australia—Senate Select Committee on Information Technologies, *In the Public Interest: Monitoring Australia's Media* (2000).

177 Ibid, recs 1–4.

178 Right to Know Coalition, *Submission PR 542*, 21 December 2007; Free TV Australia, *Submission PR 149*, 29 January 2007; SBS, *Submission PR 112*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007; Australian Press Council, *Submission PR 83*, 12 January 2007.

179 Free TV Australia, *Submission PR 149*, 29 January 2007; Australian Press Council, *Submission PR 83*, 12 January 2007.

180 Australian Press Council, *Submission PR 83*, 12 January 2007.

181 SBS, *Submission PR 112*, 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007; Australian Press Council, *Submission PR 83*, 12 January 2007.

182 Australian Broadcasting Corporation, *Submission PR 94*, 15 January 2007; Australian Press Council, *Submission PR 83*, 12 January 2007.

Among other issues, the ALRC is recommending that this review should consider the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including ACMA and the OPC.[183] There are a number of similarities between the issues impacting on the telecommunications sector and the broadcast and print media; in particular, the increasing convergence of the technology. It is outside the ALRC's Terms of Reference to recommend that this review also should cover the regulation of the broadcast and print media. The ALRC notes, however, that the Australian Government could consider the appropriateness of such an extension.

183 Rec 71–2.

43. Other Private Sector Exemptions

Contents

Introduction

43.1 A number of the major private sector exemptions from the *Privacy Act 1988* (Cth) have been examined in preceding chapters. This chapter considers the remaining private sector exemptions and partial exemptions relating to personal, family or household affairs; related bodies corporate; and changes in partnerships.[1]

Personal or non-business use

43.2 Individuals are included in the definition of an 'organisation' in the *Privacy Act*.[2] Section 7B(1) of the Act provides, however, that acts and practices of individuals are exempt if they are done *other than* in the course of business. Section 16E further provides that the National Privacy Principles (NPPs) do not apply where information is dealt with solely in the context of an individual's personal, family or household affairs. It appears from the Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) that 'personal, family or household affairs' has the same meaning as 'other than in the course of business'.[3]

---

1 This Report distinguishes between exemptions and partial exemptions to the requirements set out in the *Privacy Act*, and exceptions to the privacy principles. An exemption applies where a specified entity or a class of entity is not required to comply with any requirements in the *Privacy Act*. A partial exemption applies where a specified entity or a class of entity is required to comply with either: (1) some, but not all, of the provisions of the *Privacy Act*; or (2) some or all of the provisions of the *Privacy Act*, but only in relation to certain of its activities. An exception applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. See Ch 33.

2 *Privacy Act 1988* (Cth) s 6C(1)(a).

3 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [164].

43.3 There is no express reference to 'personal, family or household affairs' or similar wording in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines).[4] OECD Guideline 2, however, provides that the Guidelines are only intended to

> apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.[5]

43.4 The Memorandum to the OECD Guidelines goes on to state that these risks 'are intended to exclude data collections of an obviously innocent nature (for example, personal notebooks)'.[6]

43.5 Neither the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) nor the Asia-Pacific Economic Cooperation (APEC) Privacy Framework apply to the handling of personal information in connection with an individual's personal or household affairs.[7] An exemption for personal, family or household affairs also is provided for in many overseas jurisdictions, including the United Kingdom, Canada, New Zealand and Hong Kong.[8]

43.6 Privacy concerns about the exemption for personal or non-business use primarily arise in the context of developments in technology. For example, in its submissions to other inquiries into the *Privacy Act*, the Australian Privacy Foundation suggested that this exemption needs to be reconsidered due to increasing incidents of abuse, including 'inappropriate use of mobile phone cameras and misguided and extremely prejudicial "vigilante" websites'.[9] In this Inquiry, much of the concern about individuals acting in their personal capacity has related to information posted by

---

4 Privacy legislation in some overseas jurisdictions uses expressions that are similar to 'personal, family or household affairs', eg, 'personal or domestic purposes' (*Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(2)(c)); 'personal or domestic activities' (*Federal Data Protection Act 1990* (Germany) ss 1(2), 27).

5 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 2.

6 Ibid, Memorandum, [43].

7 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 3(2); Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), recital 12.

8 *Data Protection Act 1998* (UK) s 36; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4; *Privacy Act 1993* (NZ) s 56; *Personal Data (Privacy) Ordinance* (Hong Kong) s 52.

9 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.

individuals on websites, such as the posting of photographs and other personal information on websites and 'blogs'.[10]

ALRC's view

43.7 The *Privacy Act* should retain an exemption for personal and non-business use of personal information. As noted above, privacy concerns about personal or non-business use of personal information primarily arise in the context of developments in technology. In this Report, the ALRC makes a number of recommendations to improve personal information handling in the online environment. In particular, the ALRC recommends that state and territory education departments should incorporate education about privacy in the online environment into school curriculums.[11]

43.8 The ALRC also recommends introducing a statutory cause of action for serious invasions of privacy. This cause of action will apply to serious breaches of an individual's privacy arising out of personal or non-business use of personal information including, for example, where personal information is posted on an individual's website or blog.[12]

Related bodies corporate

43.9 An act or practice is not an interference with privacy if it consists of the collection or disclosure of personal information by a body corporate from or to a 'related body corporate'.[13] The stated reason for this exemption is to 'recognise [the] commercial reality that, for many bodies corporate to continue to operate effectively, they need to be able to communicate with related bodies corporate'.[14]

43.10 The partial exemption for related bodies corporate does not apply in a range of circumstances, including:

- the collection or disclosure of 'sensitive information';[15]

---

10 Confidential, *Submission PR 399*, 7 December 2007; Confidential, *Submission PR 49*, 14 August 2006. 'Blog' is a shortened form of web log. It means a record of items of interest found on the internet, edited and published as a website with comments and links; or a personal diary published on the internet: *Macquarie Dictionary* (online ed, 2007).

11 Rec 67–3.

12 See Ch 74.

13 *Privacy Act 1988* (Cth) s 13B(1). Section 6(8) of the *Privacy Act* provides that 'the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the *Corporations Act*'. A 'related body corporate' is defined in s 50 of the *Corporations Act* to mean that where a body corporate is a holding company of another body corporate, a subsidiary of another body corporate, or a subsidiary of a holding company of another body corporate, the first mentioned body and the other body are related to each other.

14 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [138].

15 *Privacy Act 1988* (Cth) s 13B(1). The definition of sensitive information is discussed in Ch 6.

- the collection of personal information from an entity that is exempt from the *Privacy Act*;[16]

- where the company is a contractor under a Commonwealth contract and: the collection or disclosure of personal information from or to the related company is contrary to a contractual provision; or the collection of personal information is for the purpose of meeting an obligation under the contract and the disclosure is for direct marketing purposes;[17] and

- if the acts and practices of the company: breach the tax file number (TFN) guidelines, or involve an unauthorised requirement or request for disclosure of an individual's TFN; contravene Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) or the data-matching guidelines made under that Act; constitute a breach of the guidelines under s 135AA of the *National Health Act 1953* (Cth); or constitute a credit reporting infringement by a credit reporting agency or a credit provider.[18]

43.11 Before an organisation can rely on this exemption to disclose non-sensitive personal information to other related companies, it must take reasonable steps to ensure that the individual knows that the organisation has collected the information, the use that will be made of the information and the types of organisations to which the information is usually disclosed.[19] In addition, although related companies may share personal information, the handling of that information is still subject to the NPPs in other respects.[20] For example, each company within the group of related companies must use the information for the primary purpose for which it was originally collected, and may use the personal information for a secondary purpose only where that purpose is allowed by NPP 2.1.[21]

43.12 The way the exemption operates may be illustrated by the following example. A large furniture store collects an individual's credit card details to receive payment for a sofa, and the individual's name and address in order to deliver the sofa. The related body corporate exemption allows the furniture store to pass on the individual's name, address and credit card details to a related delivery company. The delivery company is allowed to collect the information from the furniture company without having to inform the individual that it has collected that information. The delivery company can use this personal information only for the purpose for which the furniture store collected it (ie, delivery of the sofa). It cannot use the information for an unrelated purpose.

---

16 Ibid s 13B(1A)(a), (b).
17 Ibid s 13B(2).
18 Ibid s 13E.
19 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [139].
20 *Privacy Act 1988* (Cth), note to s 13B(1); Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [141].
21 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [141].

43.13 The related bodies corporate exemption has been criticised as a potential loophole through which corporate groups could evade the coverage of the *Privacy Act*.[22] In its submissions to previous inquiries, Electronic Frontiers Australia submitted that the exemption enables large businesses intentionally to structure their affairs to take advantage of the exemption. In its view, individuals should not have to ask or attempt to investigate corporate structures to find out how far their personal information could be spread. Electronic Frontiers Australia submitted that the exemption should be removed and related bodies corporate treated as third parties.[23]

Submissions and consultations

43.14 In submissions to this Inquiry, some stakeholders supported retaining the current exemption for related bodies corporate.[24] For example, Telstra submitted that the exemption is 'necessary for efficient and effective business practices'.[25] The Hobart Branch of the National Seniors Association Ltd also submitted that it needed to transfer personal information to related bodies, including between its national body and local branches.[26]

43.15 Other stakeholders have submitted, however, that the breadth of the exemption can result in uses of personal information which are contrary to the reasonable expectations of individuals.[27] The Cyberspace Law and Policy Centre, for example, noted that 'many corporate relationships are obscure and customers of one trading enterprise are often unaware of other ownership or control relationships'.[28] The Office of the Privacy Commissioner (OPC) submitted that organisations should inform individuals about related companies with which they regularly exchange information.[29]

43.16 Concerns also have been raised about the potential for the exemption to allow personal information to be used for direct marketing by related bodies corporate

---

22 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [9.9].

23 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; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005.

24 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Telstra, *Submission PR 185*, 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.

25 Telstra, *Submission PR 185*, 9 February 2007.

26 Hobart Branch of National Seniors Association Ltd, *Submission PR 368*, 4 December 2007.

27 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 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; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007, referring to Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005.

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

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

without an individual's knowledge or consent.[30] The ABA submitted, however, that these concerns do not relate to the related bodies corporate exemption—rather, they are about the use of personal information once it has been shared.[31]

43.17 The OPC also suggested that the *Privacy Act* should be amended to clarify that, where an organisation discloses personal information to a related body corporate in an overseas jurisdiction, that transfer will be subject to the 'Cross-Border Data Flows' principle in the model Unified Privacy Principles (UPPs).[32]

ALRC's view

43.18 In the interest of business efficacy, companies that have a shared ownership or controlling interest should be able to share non-sensitive personal information. The partial exemption for related bodies corporate is subject to a number of limitations. First, it is confined to non-sensitive personal information. Secondly, the exemption does not apply to the collection of personal information from an entity that is exempt from compliance with the *Privacy Act*. In addition, before an organisation can disclose such information to other related companies, it must take reasonable steps to ensure that individuals know the types of organisations to which the information is usually disclosed. Finally, although related companies may share non-sensitive personal information, they must otherwise comply with all the other privacy principles in the handling of that information.

43.19 The above restrictions largely limit the application of the partial exemption for related bodies corporate to transfers of personal information within the reasonable expectations of individuals. The ALRC also makes a number of recommendations in this Report to improve the transparency of information handling practices, through the 'Openness' principle and the 'Notification' principle in the model UPPs.[33] These principles may require an organisation to inform individuals about related organisations with which they regularly exchange information.[34]

43.20 One of the main issues raised about the related bodies corporate exemption is the potential for personal information to be used by a related company for the purpose of direct marketing. In Chapter 26, the ALRC recommends that organisations should be subject to a 'Direct Marketing' principle, which sets out the circumstances in which an organisation may use or disclose personal information for the purpose of direct marketing. In particular, the recommended principle provides that, where the

---

30 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171*, 5 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

31 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

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

33 See Chs 23, 24.

34 See, in particular, Rec 23–2(f).

individual is not an existing customer[35] or is under 15 years of age: the individual must have consented to the direct marketing; or the organisation must demonstrate that it was impracticable to seek such consent.[36] The organisation also must advise the individual that he or she can opt out of any further direct marketing, and provide a simple and functional means by which the individual can unsubscribe.[37]

43.21 In Chapter 31, the ALRC recommends that s 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia, the transfer will be subject to the 'Cross-Border Data Flows' principle.[38]

Change in partnership

43.22 In certain circumstances, an act or practice is not an interference with the privacy of an individual if it consists of passing personal information from an old to a new partnership.[39] The new partnership must: be formed at the same time or immediately after the old one; have at least one partner transferred from the old partnership; and carry on the same or a similar business as the old partnership.[40] The exemption applies to the disclosure and collection of personal information between the old and new partnerships, but does not apply to the use and holding of the information.[41]

43.23 The exemption does not apply if the acts and practices: breach the TFN guidelines, or involve an unauthorised requirement or request for disclosure of an individual's TFN; breach Part 2 of the *Data-matching Program (Assistance and Tax) Act* or the data-matching guidelines made under that Act; constitute a breach of the guidelines under s 135AA of the *National Health Act*; or constitute a credit reporting infringement by a credit reporting agency or a credit provider.[42]

43.24 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill gave the following example to illustrate the reason for the exemption:

> For example, a law firm (a partnership) collects personal information from, and holds personal information about, its clients. If a partner leaves the partnership, and a new partner joins the firm, the first partnership has dissolved and a second partnership forms. The purpose of clause 13C is to prevent disclosure to the second partnership

35 In Ch 26, the ALRC notes that an individual who is an 'existing customer' of a particular organisation will probably not be an 'existing customer' of a related body corporate of that organisation.
36 Rec 26–4(a).
37 Rec 26–4(b),(c).
38 Rec 31–5.
39 *Privacy Act 1988* (Cth) s 13C.
40 Ibid s 13C(1).
41 Ibid, note to s 13C(1).
42 Ibid s 13E.

> and collection by the second partnership from being an interference with privacy. The sub-clause is not intended to allow a partnership to reform and use the information collected for a totally different business purpose.[43]

43.25 Stakeholders have not raised concerns in this Inquiry about the partial exemption for changes in partnership. The OPC stated that where there is a change in partnership that falls within the exemption,

> as a matter of best practice … [the] new partnership should write to their customers and advise them of the change. In this way the individual concerned has a measure of choice over whether they wish to continue to transact with the new partnership and in this way have some control over their personal information that the partnership has collected.[44]

ALRC's view

43.26 Partnership law provides that, subject to the terms of the specific partnership agreement, an old partnership is dissolved and a new partnership is created whenever a partner joins or leaves a partnership.[45] The exemption is a sensible approach to avoid an unnecessary burden on partnerships to obtain consent from individuals for the transfer of their personal information from the old partnership to the new one each time a partner joins or leave a partnership. It should be noted that, except for the transfer of personal information from the old partnership to the new, the partnership must continue to comply with the privacy principles in all other respects.

43.27 The ALRC agrees that, as a matter of best practice, it is desirable for a new partnership to write to their customers to advise them of the change. This does not need to be a formal statutory requirement.

---

43 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [144].

44 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also: Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

45 *Partnership Act 1892* (NSW) ss 24(1)(7), 26, 32, 33; *Partnership Act 1891* (Qld) ss 27(1)(g), 29, 35, 36; *Partnership Act 1958* (Vic) ss 28(7), 30, 36, 37; *Partnership Act 1895* (WA) ss 35(6), 43, 44; *Partnership Act 1891* (SA) ss 24(1)(g), 26, 32, 33; *Partnership Act 1891* (Tas) ss 29(g), 31, 37, 38; *Partnership Act* (NT) ss 28(1)(g), 30, 36, 37; *Partnership Act 1963* (ACT) ss 29(7), 31, 37, 38.

44. New Exemptions or Exceptions

Contents

Introduction

44.1 In this chapter, the ALRC focuses on possible new exemptions and exceptions[1] from the requirements of the *Privacy Act 1988* (Cth), including in relation to alternative dispute resolution (ADR), establishing, pursuing and defending legal rights, and the information-handling practices of private investigators, insolvency administrators, valuers, professional archivists and archival organisations. In particular, the ALRC recommends new exceptions to the 'Collection' and 'Use and Disclosure' principles for the purposes of confidential ADR processes. The ALRC also

1 This Report distinguishes between exemptions and partial exemptions to the requirements set out in the *Privacy Act*, and exceptions to the privacy principles. This distinction is discussed in detail in Ch 33.

recommends that the Council of Australian Governments (COAG) should consider the regulation of private investigators and the impact of federal, state and territory laws on the industry.

44.2 In this chapter, the ALRC also discusses the partial exemption contained in Part VIA of the Act relating to declared emergencies, which came into operation in December 2006.

Alternative dispute resolution bodies

Background

44.3 ADR has been described as dispute resolution processes, other than judicial determination, in which an impartial person helps those involved in a dispute to resolve their issues.[2] ADR occurs in a broad range of settings, including services provided by

> a sole practitioner, a partnership, a for profit organisation, a not for profit organisation, as an ancillary role in an organisation whose main business is something else (including government agencies, private companies, courts and tribunals) or by an organisation established for that specific purpose under an industry scheme.[3]

44.4 The *Privacy Act* does not include an exemption or exception for ADR bodies or processes. ADR providers that fall within the definition of agency or organisation in the *Privacy Act* must operate in accordance with the Information Privacy Principles (IPPs) or National Privacy Principles (NPPs), respectively. Agencies and organisations that take part in ADR also must comply with privacy laws during the dispute resolution process.[4]

44.5 In DP 72 the ALRC asked whether the *Privacy Act* or other relevant legislation should be amended to provide exemptions or exceptions applicable to the operation of ADR schemes. Specifically, the ALRC sought views on whether the proposed:

- 'Specific Notification' principle should exempt or except ADR bodies from the requirement to inform an individual about the fact of collection of personal information, including unsolicited personal information, where to do so would prejudice an obligation of privacy owed to a party to the dispute, or could cause safety concerns for another individual;

---

2 See, National Alternative Dispute Resolution Council, *What is ADR?* (2007) <www.nadrac.gov.au agd/www/Disputeresolutionhome.nsf> at 15 May 2008. The ALRC also uses the term 'external dispute resolution' (EDR) to refer to the resolution of complaints or disputes by an entity (other than a court, tribunal or government regulator) that is external to the organisation subject to the complaint or dispute, including by EDR schemes approved by the Australian Securities and Investments Commission: see Chs 54, 59.

3 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008.

4 One minor exception to these requirements is ADR conducted by a person or persons employed by a court, which will fall within the exemption for federal courts and tribunals. This exemption is discussed in Ch 35.

- 'Use and Disclosure' principle should authorise the disclosure of personal and sensitive information to ADR bodies for the purpose of dispute resolution; and

- 'Sensitive Information' principle should authorise the collection of sensitive information without consent by an ADR body where necessary for the purpose of dispute resolution.[5]

Submissions and consultations

44.6 Stakeholders that commented on this question almost universally supported an amendment to the *Privacy Act* to provide exemptions or exceptions for ADR schemes.[6] The National Alternative Dispute Resolution Advisory Council (NADRAC), for example, commented that:

> ADR processes largely rely on the good faith of the parties to the dispute and the truthfulness of their statements … ADR processes are aimed at getting each party to outline the full context of the dispute from their perspectives with a view to identifying the underlying interests of each party … In the course of 'telling their story' many parties will include information that seems to them to be important and which may help to indicate how they came to their position but which would be deemed irrelevant in legal proceedings. The accounts will often include personal information including sensitive information about themselves and others whom the person considers to be directly or indirectly involved.[7]

44.7 The Australian Privacy Foundation supported a 'review of the application of privacy principles in the context of dispute resolution (both internal and external) with a view to justifying selective exemptions'.[8] The Department of Broadband, Communications and the Digital Economy suggested that the ALRC consult more widely before coming to a view.[9]

44.8 The Office of the Privacy Commissioner (OPC) recognised the difficulties that some NPP obligations place on the dispute resolution process and supported exceptions from the 'Use and Disclosure' principle and the 'Sensitive Information' principle. It

---

5 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 40–2.

6 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008; Suncorp-Metway Ltd, *Submission PR 525*, 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 370*, 4 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.

7 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008.

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

9 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

submitted, however, that it would not be appropriate for ADR bodies to be granted an exemption from the requirement to inform an individual about the fact of collection of personal information. It submitted that the situations where applying the principle would be problematic—where informing an individual about the fact of collection of personal information would breach an obligation of privacy owed to a party to the dispute or would cause safety concerns for another individual—were accommodated adequately in the relevant privacy principle. That is, an agency or organisation is only required to take 'reasonable steps', which may include 'no steps', to make an individual aware of personal information that has been collected about them from a third party.[10] The Cyberspace Law and Policy Centre also considered safety concerns to be addressed adequately by the exception to the 'Specific Notification' principle that is already available.[11]

44.9 The Mortgage and Finance Association of Australia suggested that 'an ADR (like a court) should be able to collect and use personal information without having to comply with the NPPs (except in relation to members of the ADR)'.[12]

44.10 A number of stakeholders addressed the potential scope of an exemption or exception for ADR. The Cyberspace Law and Policy Centre suggested that the exemption should apply to the *function* of dispute resolution, rather than being limited to ADR bodies.[13] It noted, however, that it will 'be necessary to impose some conditions on such a wide exemption to prevent abuses under the guise of internal dispute resolution'.[14] National Legal Aid also commented that the definition of an ADR scheme needed to be developed further, given the wide variety of schemes that potentially fall within this class.[15]

44.11 Some stakeholders linked exceptions to the *Privacy Act* with other legal and ethical requirements that attach to the ADR process.[16] The Recruitment and Consulting Services Association (RCSA), for example, submitted that mediators should be exempt in all circumstances where they are operating in accordance with mediation principles established under a scheme such as the LEADR Association of Dispute Resolvers (LEADR), the Institute of Arbitrators and Mediators Australia (IAMA), or schemes established by the state bar associations and law societies and institutes. The RCSA argued that the confidentiality that attaches to these schemes provided adequate

---

10 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
11 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
12 Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007.
13 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
14 Ibid.
15 National Legal Aid, *Submission PR 521*, 21 December 2007.
16 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

protection for third parties.[17] The Office of the Victorian Privacy Commissioner submitted that:

> rules concerning collection, use and disclosure of personal and/or sensitive information … would ordinarily be dealt with by the ADR practitioner's duties of confidentiality, the consent to conciliate or mediate obtained from parties to the dispute and the confidentiality agreements entered into by parties as a condition of the ADR process.[18]

44.12 The OPC suggested that, in order to provide certainty regarding the exception, those bodies that are deemed ADR bodies for the purposes of the *Privacy Act* should be set out in regulations.[19]

44.13 The Australian Bankers' Association (ABA) noted that authorising the disclosure of personal information by a bank to an ADR scheme for the purpose of dispute resolution may not overcome the bank's duty of confidentiality. It recommended, therefore, that an entity should be protected from proceedings for contravening a duty of confidence where it has disclosed personal information in accordance with an ADR exception. It was suggested that this could be modelled on the *Privacy Legislation Amendment (Emergencies and Disaster) Act 2006* (Cth).[20]

Options for reform

44.14 If adopted, the scope of an ADR exception could be clarified in a number of ways, including:

- defining ADR for the purposes of the *Privacy Act*;
- limiting the exception to specified ADR schemes or bodies; or
- limiting the exception to ADR processes that meet specified standards, for example, confidentiality requirements.

Definition of ADR

44.15 The scope of an exception to the *Privacy Act* for ADR could be qualified by including a definition of ADR processes for the purposes of the Act. An example of federal legislation that has defined ADR processes is the *Administrative Appeals Tribunal Act 1975* (Cth), which sets out a non-exhaustive list of processes that might be included within ADR:

---

17 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

18 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

20 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008. See *Privacy Act 1988* (Cth) s 80P(3).

> 'alternative dispute resolution processes' means procedures and services for the resolution of disputes, and includes
>
> (a) conferencing;
>
> (b) mediation;
>
> (c) neutral evaluation;
>
> (d) case appraisal;
>
> (e) conciliation;
>
> (f) procedures or services specified in the regulations;
>
> but does not include:
>
> (g) arbitration; or
>
> (h) court procedures or services.
>
> Paragraphs (b) to (f) of this definition do not limit paragraph (a) of this definition.[21]

44.16 Due to the diverse settings in which ADR operates, however, one commentator has stated that it is 'impossible to construct a concise definition of ADR processes that is accurate in respect of the range of processes available and the context in which they operate'.[22] NADRAC has advised that it is not generally helpful to provide definitions of ADR in legislation, except where it is proposed to: list the types of ADR that are permitted in a particular context; limit the categories or qualifications of persons authorised to carry out ADR; or provide defined circumstances for certain outcomes, such as non-admissibility on court actions.[23]

Accreditation of ADR providers

44.17 Another way of qualifying an ADR exception is by restricting its application to 'authorised' ADR providers. For example, for a corporation to be licensed to provide financial services it must have dispute resolution systems in place, including an internal dispute resolution process and membership of an external dispute resolution scheme approved by the Australian Securities and Investments Commission (ASIC).[24] Before approving dispute resolution schemes, ASIC takes into account a number of factors, including, for example, whether the scheme: reports any systemic, persistent or deliberate misconduct to ASIC; is independent from the parties to the complaint; and has appropriate published procedures.[25]

---

21 *Administrative Appeals Tribunal Act 1975* (Cth) s 3(1). This definition was inserted by the *Administrative Appeals Tribunal Amendment Act 2005* (Cth), following consultation with NADRAC. A similar approach has been adopted in the *Workplace Relations Act 1996* (Cth) s 698.

22 T Sourdin, *Alternative Dispute Resolution* (2nd ed, 2005), 2.

23 National Alternative Dispute Resolution Advisory Council, *Legislating for Alternative Dispute Resolution: A Guide for Government Policy-Makers and Legal Drafters* (2006), 29.

24 *Corporations Act 2001* (Cth) s 912A.

25 *Australian Securities and Investments Commission Act 2001* (Cth) s 21FA. ASIC has published guidelines that set out in more detail how these requirements should be met. See Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999.

44.18 Under recent amendments to the *Family Law Act 1975* (Cth), all family dispute resolution practitioners must be accredited under the Accreditation Rules or be authorised by an organisation designated by the Attorney-General or a designated court.[26] All individuals applying for accreditation also must have access to a complaints process. Accredited practitioners are publicly listed on the Family Dispute Resolution Register.[27]

44.19 On 1 January 2008, the National Mediator Accreditation System—a voluntary accreditation system for mediators—commenced. Under the system, Recognised Mediator Accreditation Bodies accredit mediators, where they meet set training and education standards in addition to ongoing practice and competency requirements.[28] ADR providers also may be accredited through professional associations, such as the LEADR and IAMA.

Requirements of confidentiality

44.20 Confidentiality obligations are another way of limiting the scope of an ADR exception under the *Privacy Act*. Requirements for confidentiality often are contained in a contractual agreement entered into by the parties and the provider. For example, the LEADR Model Mediation Agreement provides:

> The Parties and the Mediator will not unless required by law to do so, disclose to any person not present at the Mediation, nor use, any confidential information furnished during the Mediation unless such disclosure is to obtain professional advice or is to a person within that Party's legitimate field of intimacy, and the person to whom the disclosure is made is advised that the confidential information is confidential.[29]

44.21 Confidentiality conditions also may be set out in legislation. The *Family Law Act*, for example, provides that 'a family dispute resolution practitioner must not disclose a communication made to the practitioner while the practitioner is conducting family dispute resolution, unless the disclosure is required or authorised under [the Act]'.[30] The *Evidence Act 1995* (Cth) prevents evidence from being adduced where it is connected to a settlement negotiation between persons in dispute and a third party.[31]

---

26 *Family Law Act 1975* (Cth) s 10G. Interim Accreditation Rules were implemented in the *Family Law Amendment Regulations 2007 (No. 1)* (Cth).

27 Australian Government Attorney-General's Department, *Registration Process for Family Dispute Resolution Providers* <www.ag.gov.au> at 14 February 2008.

28 T Sourdin, *Australian National Mediator Accreditation System: Report on Project* (2007).

29 LEADR Association of Dispute Resolvers, *Mediation Agreement* <www.leadr.com.au> at 11 February 2008, cl 19.

30 *Family Law Act 1975* (Cth) s 10(H). Disclosure is permitted in some circumstances, such as with consent, in order to prevent or lessen a risk of harm, or to report the commission of certain offences.

31 *Evidence Act 1995* (Cth), s 131.

44.22 Confidentiality of ADR processes also may be inferred at common law.[32] This inference, however, is not self-evident. In *Esso Australia Resources Ltd v Plowman (Minister for Energy and Minerals)*, for example, the High Court held that there was no implied term in an agreement to arbitrate preventing parties from disclosing information provided in and for the purposes of arbitration. Confidentiality only applied to documents produced compulsorily.[33] The scope of confidentiality protections also varies—for example, although the ADR provider generally will be bound by obligations of confidentiality, this often will not extend to the parties to the dispute. NADRAC has noted that

> in the absence of any overarching legislative or common law requirement [for confidentiality] … it is impossible for NADRAC to say either that confidentiality is always maintained or that information revealed in the dispute resolution process is never used for other purposes.[34]

ALRC's view

44.23 Australian society is increasingly recognising the integral role that ADR plays in the effective, efficient and fair resolution of disputes. This is reflected by its integration both into the formal justice system—by making referral of disputes to ADR mandatory and access to legal aid and advice contingent on a requirement to try ADR—and more broadly across the community and commercial sectors. In this Inquiry, the ALRC recommends a greater role for industry-based ADR schemes in the resolution of complaints about credit reporting.[35]

44.24 The resolution of disputes through ADR is facilitated by the disclosure of all relevant information by the parties to dispute resolution bodies, including personal information about third parties. As NADRAC has noted,

> in a web of social interaction, the affairs of one person will be inextricably linked to the affairs of others. Disputes between some members of a community will frequently be linked to the conduct of others, and resolution of those disputes will often rely on the sharing of information that relates to others.[36]

44.25 The *Privacy Act* has the potential to present significant barriers to this information exchange. Under the 'Collection' principle, agencies and organisations providing ADR services may be prevented from collecting sensitive personal information about third parties where it does not have that person's consent. Similarly, under the 'Use and Disclosure' principle, an agency or organisation that is participating in the dispute resolution process may be prevented from disclosing personal information relating to third parties. It also may be prevented from disclosing sensitive personal information that relates to a party to the dispute if that person withholds

---

32 See, eg, *AWA Ltd v George Richard Daniels* (1992) 7 ACSR 463 (Comm Div).
33 *Esso Australia Resources Ltd v Plowman (Minister for Energy and Minerals)* (1995) 183 CLR 10.
34 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008.
35 See Ch 59.
36 National Alternative Dispute Resolution Advisory Council, *Submission PR 564*, 23 January 2008.

consent. This may occur, for example, where the information could undermine that party's position.

44.26 The ALRC recommends, therefore, that agencies and organisations be permitted to use and disclose personal information under the 'Use and Disclosure' principle; and to collect sensitive information under the 'Collection' principle, where the collection, use or disclosure is necessary for the purpose of an ADR process.

44.27 Another concern is the need to make individuals aware of certain information upon collection of personal information about them. In some situations, it may be impracticable for an agency or organisation that is providing ADR services to notify third parties that personal information about them has been collected during a dispute resolution process. This may be the case, for example, where it would breach an obligation of confidentiality owed to a party to the dispute or would cause safety concerns for another individual. The ALRC is recommending a broader change to the 'Notification' principle to make clear that 'reasonable steps' to make an individual aware that personal information about him or her has been collected from a third party may include taking no steps.[37] This change will accommodate sufficiently the concerns of agencies and organisations providing ADR services.

44.28 One objection that could be raised about the ALRC's recommendation that the 'Collection' principle and the 'Use and Disclosure' principle should include specific exceptions for the purpose of ADR is the potential for similar issues to arise in other contexts. For example, an agency or organisation that provides a counselling service or is involved in complaint handling also may need to collect sensitive personal information about third parties. The ALRC did not receive any submissions raising these concerns, however, and has not had an opportunity to consult on the potential ramifications of any such additional exceptions. While this may be an issue that can be explored further when the recommendations are considered, the ALRC has not made a recommendation to expand the ADR exceptions to other contexts.

Limiting the scope of the principle

44.29 As noted above, without further qualification, ADR potentially could include an extremely broad range of situations. Depending on the other information-handling practices associated with the ADR process, this has the potential to result in misuse of the information used or disclosed in accordance with the exceptions. This is a particular concern where the individual or body providing the ADR service falls outside the definition of 'organisation' or 'agency', and therefore is not required to

37 The 'Notification' principle is discussed in Ch 23.

comply with the Act.[38] Individual participants also are outside the requirements of the *Privacy Act*.

44.30 The ALRC considers confidentiality requirements to be the most appropriate way of containing personal information shared through the recommended ADR exceptions. That is, provided that the parties to the dispute and the ADR provider are bound by relevant confidentiality obligations—whether these be through contractual agreements or legislative provisions—any personal information that is collected, used or disclosed for the purpose of dispute resolution will remain limited to that domain unless there is express consent of the parties or another relevant exception applies. For example, an agency or organisation that has provided ADR services may be required to disclose personal information where it is connected to suspected child abuse. It also may be appropriate to extend confidentiality obligations to prevent the disclosure of personal information about a third party without the consent of that person.

44.31 The ALRC recommends that the exceptions to the 'Collection' principle and the 'Use and Disclosure' principle extend only to 'confidential' dispute resolution processes. What constitutes confidentiality requirements in particular ADR settings should be articulated in the OPC's guidance on information handling in the context of ADR. The OPC should consult with NADRAC when formulating this guidance.

44.32 Agencies and organisations that engage in dispute resolution processes also may be required to comply with the other components of the *Privacy Act*. This will provide additional protection for personal information collected, used and disclosed in an ADR process. For example, where personal information—either relating to a party to the dispute or to a third party—is disclosed for the purpose of the dispute resolution process, the 'Use and Disclosure' principle prevents this information from being used or disclosed for any other purpose. When the information is no longer relevant for the purpose of dispute resolution, the 'Data Security' principle requires that it must be destroyed or rendered non-identifiable.[39]

44.33 Provided the confidentiality safeguards are in place, it is unnecessary to stipulate an additional requirement that agencies or organisations providing ADR must be 'authorised'. The practical application of such a requirement would give rise to a number of problems. Those accreditation systems that are presently operating only cover a specific ADR process (such as mediation) or a particular context (such as financial services disputes). Limiting the exceptions to those agencies or organisations that fall within one of these schemes would artificially fragment the application of the exceptions. The alternative accreditation option—that is, introducing a new accreditation system for the purpose of the *Privacy Act*—would involve a heavy administrative burden. It is also unclear what the criteria should be for such

38 Many ADR providers presently fall within the small business exemption. This exemption, including a recommendation that it be removed, is discussed in Ch 39.

39 The 'Data Security' principle is discussed in Ch 28.

accreditation, and who should be responsible for the administration of the accreditation system.

44.34 Finally, by its very nature, ADR is dynamic and diverse. Provided the confidentiality safeguards outlined above are in place, this diversity should be accommodated. This is best managed by applying the exception to the broad ambit of ADR processes.

Recommendation 44–1 The *Privacy Act* should be amended to provide an exception to the:

(a) 'Collection' principle to authorise the collection of sensitive information, and

(b) 'Use and Disclosure' principle to authorise the use and disclosure of personal information,

where the collection, use or disclosure by an agency or organisation is necessary for the purpose of a confidential alternative dispute resolution process.

Recommendation 44–2 The Office of the Privacy Commissioner, in consultation with the National Alternative Dispute Resolution Advisory Council, should develop and publish guidance on what constitutes a confidential alternative dispute resolution process for the purposes of the *Privacy Act*.

Establishing, pursuing and defending legal rights

Background

44.35 A number of submissions to this Inquiry—in particular, those from private investigators and related industry associations—commented on the impact of privacy laws on the ability of individuals to establish, pursue or defend legal rights, such as in debt recovery.[40] The Australian Investigators Association, for example, commented that:

> The inability to locate a contact address for an individual who is a witness to an incident such as an accident, fraud or other crimes essentially amounts to a denial of

40 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; R Lake, *Submission PR 305*, 19 July 2007.

> natural justice for the affected parties (defendants) as an investigator cannot complete his or her tasks unless the witness is located.[41]

44.36 One commercial investigator advised that he frequently acts in matters where law enforcement or regulatory agencies have declined to investigate based on commercial considerations.[42] He noted a speech by Nicholas Cowdrey QC (the New South Wales Director of Public Prosecutions), where he stated that frauds below a certain threshold— potentially including frauds of a value of $10,000—will generally not be investigated by the police.[43]

44.37 The issue also was raised by a small business owner who rents out household whitegoods:

> Many of our customers are recipients of Centrelink benefits … Unfortunately, we are finding that a number of these people are paying their rent through Centrepay, for a short time, and then disappearing with our goods. Naturally, we attempt to trace these people, but due to the *Privacy Act*, we are given no assistance by Centrelink. The last two days have been spent on the telephone trying to find someone who can help us, all to no avail. Every person spoken to continually refers to the *Privacy Act*.[44]

44.38 There is no general exemption from the requirements of the *Privacy Act* for the purpose of establishing, pursuing or defending a legal claim. Some of the exceptions to the privacy principles, however, are of relevance. An organisation may collect sensitive information where 'the collection is necessary for the establishment, exercise or defence of a legal or equitable claim'.[45] In addition, some of the exceptions to the 'Use and Disclosure' principle could be relied upon by an organisation seeking to establish, pursue or defend its own legal claim against the individual to whom the information relates.[46]

44.39 These provisions, however, do not cover the situation where an agency or organisation is asked to disclose personal information about a third party in order to further a third party's legal claim. This is in contrast to the United Kingdom, where the *Data Protection Act 1998* (UK) excepts personal information from the non-disclosure provisions

> where the disclosure is necessary—
>
> (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
>
> (b) for the purpose of obtaining legal advice,

---

41 Australian Investigators Association, *Submission PR 507*, 21 December 2007.
42 R Lake, *Submission PR 305*, 19 July 2007.
43 Ibid.
44 J Tozzi-Condivi, *Submission PR 438*, 10 December 2007.
45 *Privacy Act 1988* (Cth) sch 3, NPP 10.1(e). Non-sensitive personal information can be collected under the general provision that the information is 'necessary for one or more of its functions or activities': *Privacy Act 1988* (Cth) sch 3, NPP 1.1.
46 See discussion in Ch 25.

> or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.[47]

Other processes to obtain personal information

44.40 Personal information that is necessary for the purpose of establishing, pursuing or defending legal rights may be available other than through an exception to the *Privacy Act*. In particular, information may be obtained through the courts.

44.41 Through the discovery process, parties to litigation have the opportunity to obtain information relevant to the dispute. Although discovery is generally limited to a procedure between the parties, courts also may order third parties to make available information. For example, courts may allow intending litigants to obtain information that will help them to identify a prospective defendant. This can be illustrated by Order 15A of the *Federal Court Rules 1979* (Cth), which provides:

> Where an applicant, having made reasonable inquiries, is unable to ascertain the description of a person sufficiently for the purpose of commencing a proceeding in the Court against that person … and it appears that some person has or is likely to have knowledge of facts, or has or is likely to have or has had or is likely to have had possession of any document or thing, tending to assist in such ascertainment, the Court may make an order [that the person attend before the court or make discovery of the relevant document].[48]

44.42 The 'description' of a person includes (among other information) their name, place of residence, place of business, occupation and sex.[49] Information about the identity of a prospective defendant also can be obtained in equity.[50]

44.43 Freedom of information legislation can sometimes provide another avenue through which individuals can obtain information to establish, pursue or defend legal rights. For example, an individual could apply to the state or territory register of vehicles for information on the registered operator of a vehicle.[51]

ALRC's view

44.44 There are clear public policy interests in individuals being able to establish, pursue and defend legal rights. If the application of the *Privacy Act* is preventing individuals from obtaining the necessary information to assert their legal rights, then

---

47 *Data Protection Act 1998* (UK) s 35(2).

48 *Federal Court Rules 1979* (Cth) O 15A r 3.

49 Ibid o 15A r 1. Similar rules are in place in certain courts in New South Wales, Tasmania, Victoria, Western Australia, the ACT and the Northern Territory.

50 Court orders to this effect are commonly referred to as 'Norwich orders', referring to the precedent established in the case of *Norwich Pharmacal Co v Commissioners of Customs & Excise* [1974] AC 133.

51 *Roads & Traffic Authority of NSW v Australian National Car Parks Pty Ltd* [2007] NSWCA 114. This is limited, however, as freedom of information laws include an exemption for documents that would involve the unreasonable disclosure of personal information.

changes may be justified. One way in which to do this is through an exception to the 'Use and Disclosure' principle along the lines of s 35(2) of the *Data Protection Act* (UK)—that is, where use or disclosure is necessary for the purposes of establishing, exercising or defending legal rights.

44.45 It is not apparent, however, that adding an exception to this effect would substantially improve the position of intending litigants. To fulfil the requirements of the exception, an agency or organisation must be satisfied that disclosing the information is 'necessary' for the above purposes. This requirement will be very difficult to meet in the absence of a court order. Furthermore, the provision functions only as an exception to *permit* the disclosure of information—it does not compel disclosure by an agency or organisation.

44.46 The United Kingdom Information Commissioner's Office has issued legal guidance on the *Data Protection Act*, which confirms that a data controller is not obliged to disclose personal data following a request by a third party, despite the existence of the exception for the purposes of establishing, exercising or defending legal rights. It advises:

> In many cases, the data controller will not be in a position to make a decision as to whether the necessity test can be met, or will not wish to make the disclosure because of his relationship with the data subject, with the result that the requesting party will have to rely upon a Court order to obtain the information.[52]

44.47 Processes are in place through court orders to obtain information in the course of establishing, exercising or defending legal rights. Court processes also have well established rules to prevent abuse by the parties. For example, an employer may request another organisation with which it has a business relationship to provide information on an employee's purchasing activities to see if the employee is misappropriating funds. Without some evidence that misappropriation was, in fact, occurring, courts would consider this to be a 'fishing expedition' and, therefore, impermissible.[53] This safeguard potentially could be bypassed through an exception to the 'Use and Disclosure' principle for the purpose of pursuing a legal claim.

44.48 Judicial discretion also plays an integral role in court orders for discovery against third parties. That is, for each application, the requirements of justice to the applicant will be balanced against the respondent's justification for non-disclosure.[54] Commentators have noted that this discretion provides 'an appropriate brake on any

---

52 United Kingdom Government Information Commissioner's Office, *Data Protection Act 1998 Legal Guidance* (2001), 69.

53 In this context, a 'fishing expedition' refers to seeking discovery of documents in the hope that they will reveal relevant evidence without any ground for believing that such evidence exists.

54 *Norwich Pharmacal Co v Commissioners of Customs & Excise* [1974] AC 133, 175.

excesses in the use of the Order'.[55] Indeed, it has been questioned whether an agency should ever disclose personal information, except on the order of a court.[56]

44.49 The ALRC acknowledges the potential drawbacks to requiring an individual to commence court proceedings in order to obtain personal information that he or she needs in order to establish, pursue or defend his or her legal rights. In particular—depending upon the court in which proceedings are commenced—this can be both costly and time-consuming. Court orders made in accordance with established rules, however, are the most authoritative way to secure disclosure. In light of the potential for abuse, as well as its likely limited usefulness, the ALRC does not recommend the introduction of a new exception or exemption from the *Privacy Act* for the purpose of establishing, pursuing and defending legal rights.

Private investigators

Background

44.50 Private investigators provide investigative and legal support services to government agencies, corporate entities and the public in areas that include: fraud prevention, detection, assessment and resolution; corporate fraud and risk management services; insurance fraud and claims investigation, monitoring and assessment; aviation accident and loss investigation; marine loss investigations; occupational health and safety incident investigation; witness location and skip tracing; criminal investigations; child protection investigations; investigative journalism; family law investigations; intellectual property protection services; background checking; consumer investigations; and missing person investigations.[57]

44.51 The *Privacy Act* makes no specific provision for the activities of private investigators. Private investigators are generally required to comply with the NPPs, even where they are small businesses—the small business exemption does not apply to organisations that trade in personal information.[58]

44.52 Various aspects of the operation of the *Privacy Act* have been identified as hampering the activities of private investigations, including: the obligation under NPP 1.5 to take reasonable steps to make individuals aware that information is being

---

55 B Kremer and R Davies, 'Preliminary Discovery in the Federal Court: Order 15A of the Federal Court Rules' (2004) 24 *Australian Bar Review* 235.

56 See the comments of Viscount Dilhorne to this effect: *Norwich Pharmacal Co v Commissioners of Customs & Excise* [1974] AC 133, 190.

57 Australian Institute of Private Detectives Ltd, *Code of Practice for Private Investigators in Australia* (2005), 5.

58 To trade in personal information is to collect personal information about another individual from, or disclose such information to, anyone else for benefit, service or advantage (unless it occurs with the consent of the individuals concerned, or is authorised or required by law): *Privacy Act 1988* (Cth) s 6D(7), (8).

collected about them; and the application of the 'Use and Disclosure' principle in NPP 2, which may prohibit organisations from disclosing information—including information necessary for debt collection, service of legal process, and fraud investigation—to private investigators.

44.53 A particular concern that has been raised in this Inquiry by private investigators and their representative associations is that, while the *Privacy Act* facilitates access to personal information by law enforcement bodies, no such access is available to private investigators, including those who may be engaged by defendants or others who are subject to law enforcement action. As discussed above, the ALRC does not consider a general exception that allows for disclosure of personal information for the purposes of establishing, pursuing or defending legal rights to be appropriate. Further consideration is given here to the more specific situation of private investigators.

Regulatory framework

44.54 Most states and territories have statutory schemes for licensing private investigators. Licences are granted in New South Wales, Victoria, Queensland, Western Australia, South Australia, Tasmania and the Northern Territory.[59] At present, the ACT does not require private investigators to be licensed.[60]

44.55 In New South Wales, for example, the *Commercial Agents and Private Inquiry Agents Act 2004* (NSW) establishes the regulatory framework for commercial agents and private inquiry agents. Under the Act, the Commissioner of Police issues licences to business owners (master licences) and their employees (operator licences) who undertake commercial agent or private inquiry agent activities.[61] The legislation provides for:

- Threshold requirements for granting a licence—including Australian citizenship, minimum age and an absence of convictions for 'major offences'[62] and, for master licence applicants, compliance with the requirements of any approved industry association and an absence of bankruptcy.

- Discretionary considerations for granting a licence—including appropriateness or fitness to hold a licence, previous convictions or findings of guilt for 'minor

---

59 *Commercial Agents and Private Inquiry Agents Act 2004* (NSW); *Private Agents Act 1996* (Vic); *Security Providers Act 1993* (Qld); *Security and Investigation Agents Act 1995* (SA); *Security and Related Activities (Control) Act 1996* (WA); *Security and Investigations Agents Act 2002* (Tas); *Commercial and Private Agents Licensing Act 1979* (NT).

60 However, other parts of the security industry are regulated through the *Security Industry Act 2003* (ACT).

61 See *Commercial Agents and Private Inquiry Agents Act 2004* (NSW) pt 2. The *Commercial Agents and Private Inquiry Agents Act* has been used as the basis for the draft bill prepared by the Australian Institute of Private Detectives (AIPD) to indicate how uniform national regulation of private investigation might be enacted. See Australian Institute of Private Detectives, *Private Investigators Bill 2005* <www.aipd.com.au> at 15 May 2008.

62 As defined in s 4.

offences',[63] and public interest considerations. Applications also may be refused where the prospective licensee does not meet set training or qualification requirements.

- Licensing offences—including offences in relation to: practising without a licence; failing to produce a licence on demand; employing an unlicensed person to carry out commercial agent or private inquiry work; and disposing of licences through sale, loan or gift.

44.56 A number of the regulatory features set out in the New South Wales legislation are common throughout the state and territory schemes. There are also some key differences, however, including the nature of offences that automatically disentitle an applicant from holding a licence; qualifications and training requirements; and penalties for licensing offences.

44.57 There is some movement towards harmonisation of the regulation of private investigators. Regulation of the security industry, including private investigators, has recently been considered by the Council of Australian Governments (COAG), as a part of its review of Australia's counter-terrorism arrangements. This included consideration of national standards for the security industry, such as training, accreditation, competency, registration and licensing requirements.[64] A proposed national standard for the regulation of the private security industry was presented to COAG at its meeting of 13 April 2007; however, no agreement was reached at this time.[65]

44.58 Several states have introduced or proposed legislation responding to COAG's call for harmonisation of licensing regimes for the security industry. The *Security Providers Amendment Act 2007* (Qld), for example, expands the categories of activities that are subject to its provisions, tightens probity checking of prospective licensees, increases the penalties for operating without a licence or engaging unlicensed personnel, and provides for the introduction of a mandatory code of practice and ongoing industry-based training.[66] As of February 2008, reforms to the regulation of the security industry in Western Australia were before the Legislative Council.[67]

---

63 As defined in s 4.

64 Council of Australian Governments, *Council of Australian Governments' Communiqué Special Meeting on Counter Terrorism*, 27 September 2005.

65 Council of Australian Governments, *Council of Australian Governments' Communiqué*, 13 April 2007. The areas of counter-terrorism or security are not on COAG's 2008 work agenda: Council of Australian Governments, *Council of Australian Governments' Communiqué*, 20 December 2007.

66 *Security Providers Amendment Act 2007* (Qld). At the time of writing, no code of conduct or training program had been introduced.

67 Security and Related Activities (Control) Amendment Bill 2007 (WA). The Bill was passed by the Legislative Assembly on 22 November 2007.

44.59 Private investigators also may be subject to various industry self-regulatory schemes. For example, the Australian Institute of Private Detectives (AIPD) requires its members to be bound by an AIPD Code of Practice, Code of Ethics, standards and guidelines.[68] The only sanction for a breach of these requirements, however, is the cancellation a person's membership. The AIPD does not have any power to remove a person's licence to practise as a private investigator.

Options for reform

44.60 If privacy laws impact unduly on the functions of private investigators, there are a number of options for reform. First, a specific exemption or exceptions for private investigators could be inserted into the Act. An alternative is to clarify the application to private investigators of the generally available exceptions to the privacy principles.

Exemptions or exceptions to the Privacy Act

44.61 A possible reform would be to amend the definition of 'enforcement body' in s 6 of the *Privacy Act* to include private investigators in relation to matters before courts or tribunals.[69] The effect of this would be to allow disclosure of personal information to a private investigator where disclosure is reasonably necessary for the preparation for proceedings before a court or tribunal.

44.62 There is some precedent for including private investigators within a law enforcement exception to privacy legislation. Under the Canadian *Personal Information Protection and Electronic Documents Act 2000* (PIPED Act),[70] for example, private investigators are included within the exception for investigative bodies provided they meet certain requirements, including having a privacy code that is compliant with the relevant standard and being a member in good standing of a professional association with such a code.[71] This exception has a relatively narrow scope, permitting the exchange of personal information without consent for investigative purposes between or among private organisations only in circumstances where obtaining consent is impossible, impractical or undesirable because it would frustrate the conduct of the investigation.[72]

Accommodation of private investigators under the present privacy framework

44.63 Some of the concerns raised by private investigators about the *Privacy Act* may be overcome by a better understanding of its application to their functions, both within the private investigation industry and the agencies and organisations with which they

---

68 Australian Institute of Private Detectives Ltd, *Code of Practice for Private Investigators in Australia* (2005), 22.

69 This reform was submitted for consideration by the AIPD to the OPC Review: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 229.

70 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada).

71 *Regulations Specifying Investigative Bodies 2000* SOR/2001–6 (Canada).

72 Government of Canada, 'Regulatory Impact Analysis Statement for Regulations Amending the Regulations Specifying Investigative Bodies', *Canada Gazette*, 21 April 2004.

deal. For example, one concern for private investigators is the obligation, under NPP 1.5, to take reasonable steps to make individuals aware that a private investigator is collecting information about them. In this context, the OPC has noted that the 'reasonable steps' required by the privacy principle could include taking no steps, where, for example, a suspicion of fraud or unlawful activity is being investigated.[73]

44.64 However, where investigators are investigating activity that is 'improper rather than unlawful'—for example, 'misuse of employer resources, abuse of power or position, or marital infidelity'—complying with the collection principle 'may impinge on the activities of private investigators'.[74] The OPC has observed that:

> it is considerably less clear in these circumstances that the public interest in investigating possibly improper activity outweighs the individual and the public interest in individuals being aware that they are under investigation.[75]

44.65 Where private investigation services are engaged directly by an agency or organisation, that agency or organisation also could gain consent to a range of information sharing practices.[76] For example, the notice given by an insurance company at the time that a customer takes out a policy or at the time that a customer makes a claim could include private investigators within its description of the entities to which it may disclose personal information.[77] This approach was suggested by the OPC in its *Review of the Private Sector Provisions of the Privacy Act 1988* (the OPC Review).[78] Its use was illustrated in the case of *O v Insurance Company*, in which an insurance company investigated a worker's compensation claim through a private investigator.[79] The Privacy Commissioner found that information gathered by the private investigator was a part of a lawful investigation into the factors affecting the complainant's return to work.

Submissions and consultations

44.66 In DP 72, the ALRC acknowledged the legitimate role that private investigators play in providing investigative and legal support services, but did not consider there to be sufficient accountability and oversight mechanisms in relation to the industry to justify an exemption (or other special provisions) from the operation of the *Privacy Act*. The ALRC asked whether the Australian Government should request that the Standing Committee of Attorneys-General (SCAG) consider the regulation of private

---

73 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 225.

74 Ibid, 226.

75 Ibid, 226. The 'Collection' principle is discussed in Ch 21.

76 The 'Specific Notification' principle is discussed in Ch 23.

77 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 231.

78 Ibid, 231.

79 *O v Insurance Company* [2007] PrivCmrA 17.

investigators and the impact of federal, state and territory privacy and related laws on the industry.[80]

44.67 Private investigators and related industry associations did not comment specifically on the ALRC's question but submitted further on the negative impact that privacy laws have on their functions; in particular, on their role in the legal process.[81]

44.68 The majority of stakeholders that responded to this question either specifically supported consideration of the regulation of private investigators by SCAG,[82] or commented that they saw the need for greater clarity and consistency in the regulation of the information-gathering practices of private investigators.[83]

44.69 Some stakeholders supplemented their support for further consideration with views on their preferred outcome. The Public Interest Advocacy Centre and National Legal Aid commented that—although they supported a review by SCAG—they did not consider that private investigators should be exempt from the *Privacy Act*.[84] The Investment and Financial Services Association, on the other hand, submitted that:

> the insurance industry relies upon the activities of private investigators to assist in reducing fraudulent claims and consequently would be opposed to any restrictions on their ability to provide this legitimate investigative role for the industry.[85]

44.70 The South Australian Government objected to the statement that private investigators are not accountable, at least in the case of South Australia. It advised that the *Security and Investigation Agents Act 1995* (SA) provides for disciplinary action against an agent if he or she acts unlawfully, improperly, negligently or unfairly in the course of work as an agent or is not a fit and proper person to hold a licence.[86] It commented that

> given that States and Territories license agents to carry out private investigations, it must follow that this is a proper occupation and that the activities within the purview of the licence should not be impeded by the Act.[87]

---

80 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 40–1.

81 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; R Lake, *Submission PR 305*, 19 July 2007.

82 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

83 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007.

84 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007.

85 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

86 Government of South Australia, *Submission PR 565*, 29 January 2008.

87 Ibid.

44.71 Although the South Australian Government accepted that the matter could be referred to SCAG, it suggested that it could be dealt with more simply by the list of 'non excluded matters',[88] at least with regard to those agents to whom a statutory discipline regime applies.[89]

44.72 The ABA did not support a referral to SCAG 'as it could lead to separate regulation or alternate regulation of the privacy aspects of private investigators outside of the Privacy Act'.[90] A few stakeholders submitted that there was no need for any special review of the impact of privacy laws on private investigators, who should remain subject to all the principles.[91]

ALRC's view

44.73 Private investigators have a legitimate role in providing investigative and legal support services in a range of contexts. There is, for example, a social interest in individuals being able to take effective action to recover debts owed to them, find a person who is at fault in a car accident, and prepare a case for court proceedings. In some instances, private investigators may perform tasks that could be done by the police or other law enforcement bodies if resources and priorities permitted. This role is often dependent on an ability to obtain access to personal information. The ALRC recognises that the *Privacy Act*, and state and territory privacy legislation, may present obstacles to private investigators in obtaining personal information.

44.74 The ALRC, however, agrees with the conclusion of the OPC Review that, as the industry presently stands, it is difficult to recommend that private investigators be accorded similar access rights to personal information as law enforcement agencies.

> Private detectives can be distinguished from other enforcement bodies on the basis that they are not accountable to the government or the community, or any accountability body such as an ombudsman who can investigate complaints and award compensation, in the same way that law enforcement agencies are.[92]

44.75 Comprehensive regulatory structures are required before any exemption or exceptions is granted to the private investigation industry, particularly in light of the potential for unethical and unlawful behaviour. A recent report by the Information Commissioner's Office in the United Kingdom, for example, noted that companies and individuals that unlawfully obtain confidential personal information 'are almost

---

88 The ALRC is recommending that the *Privacy Act* should not apply to a law of a state or territory so far as the law deals with any 'preserved matters': see Rec 3–3.

89 Government of South Australia, *Submission PR 565*, 29 January 2008.

90 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

91 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

92 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 230.

invariably part of the private investigation industry'.[93] Unscrupulous information brokerage by the private investigation industry has been illustrated further by the high profile United States case of *Remsburg v Docusearch Inc*.[94] No comparable Australian cases, however, were brought to the ALRC's attention in this Inquiry.

44.76 Some recognition of the private investigation industry might be justified if it were regulated more stringently. Currently, however, such recognition is premature. A broad spectrum of stakeholders agreed that a review of the regulation of private investigators and the impact of federal, state and territory privacy and related laws on the industry would be beneficial. In particular, stakeholders acknowledged the need for greater clarity and consistency in the regulation of the information-gathering practices of private investigators. Although private investigators did not make a submission on this issue, research reported in 2001 concluded that the industry would support 'tougher licensing, especially in pre-service training requirements' in return for an enhanced capacity to access information relevant to investigations.[95]

44.77 Before Industry Canada accepted private investigators as an 'investigative body' for the purposes of PIPEDA it assessed:

- the operational structure of the body or process, including identified responsibility and accountability centres;
- specific legal regimes, licensing requirements, regulations or oversight mechanisms to which the body is subject, including sanctions or penalties for non-compliance;
- the privacy protection policies or procedures followed by the body; and
- the amount of information provided to individuals about the existence and operation of the body and how to make a complaint or seek redress.[96]

44.78 In DP 72, the ALRC suggested that SCAG may be the appropriate body to review the regulation of the private investigation industry. Ministerial responsibility for oversight of private investigators varies, however, with responsibility vested in ministers for police,[97] community affairs,[98] and attorneys-general.[99] As SCAG's focus

---

93 United Kingdom Government Information Commissioner's Office, *What Price Privacy? The Unlawful Trade in Confidential Personal Information* (2006), 21.

94 In this case, a stalker obtained a young woman's personal information from an internet-based private investigation service and used this information to locate and murder the woman. *Helen Remsburg, Administratrix of the Estate of Amy Lynn Boyer v Docusearch Inc* 816 A 2d 1001 (Supreme Court of New Hampshire, 2003).

95 T Prenzler, *Private Investigators in Australia: Work, Law, Ethics and Regulation* (2001) Criminology Research Council, 6.

96 Government of Canada, 'Regulatory Impact Analysis Statement for Regulations Amending the Regulations Specifying Investigative Bodies', *Canada Gazette*, 21 April 2004.

97 In New South Wales, Victoria, Western Australia.

is directed towards matters within the portfolio responsibilities of its members,[100] private investigators may not come within its scope. COAG, therefore, is the appropriate body to review the regulation of private investigators. This is appropriate given the recent inclusion of the private security industry on COAG's agenda.

44.79 The application of the *Privacy Act* to the functions of private investigators also can be assisted by clarifying the range of ways that its requirements can be satisfied. For instance, where a private investigator acts as an agent of an agency or organisation, this could be set out in the agency's or organisation's Privacy Policy.[101] Under the 'Notification' principle, 'reasonable steps' to inform an individual that personal information about them has been collected might, in some circumstances, equal 'no steps'.[102] This often would be the case in the context of private investigators. The clarification of the *Privacy Act*'s provisions is an overriding objective of this Inquiry and the focus of numerous recommendations. These measures will accommodate sufficiently the situation of private investigation and, therefore, there is no need for further guidance in this context.

Recommendation 44–3 The Australian Government should recommend that the Council of Australian Governments consider models for the regulation of private investigators and the impact of federal, state and territory privacy laws on their operations.

Insolvency practitioners

44.80 In its submission on DP 72, the Insolvency Practitioners Association of Australia (IPAA) advised that privacy laws were impacting adversely on the conduct of insolvencies. In particular, the IPAA commented that the *Privacy Act* was hindering: the collection of information in connection with the investigatory functions of insolvency practitioners; and the disclosure of insolvency information to creditors and other interested parties.[103]

98 In South Australia.

99 In Queensland, Tasmania, Northern Territory.

100 Australian Government Attorney-General's Department, *Standing Committee of Attorneys-General* <www.ag.gov.au> at 14 April 2008.

101 In Ch 24, the ALRC recommends a system whereby agencies and organisations create a 'Privacy Policy' setting out their polices on the management of personal information and how personal information is collected, held, used and disclosed.

102 The obligation on agencies and organisations to notify an individual whose personal information has been, or is to be, collected—including the situation where taking 'reasonable steps' equates with taking 'no steps'—is considered in Ch 23.

103 Insolvency Practitioners Association, *Submission PR 404*, 7 December 2007.

44.81 Under the *Corporations Act 2001* (Cth) and the *Bankruptcy Act 1966* (Cth), insolvency practitioners have extensive powers of investigation and inquiry to determine the circumstances of insolvencies.[104] The IPAA submitted that when its members make an inquiry it is not uncommon for agencies or organisations to withhold the information on the basis of the *Privacy Act*. The practitioner is then required to use a formal demand process to obtain the information.[105]

44.82 Insolvency practitioners disclose personal information in order to inform creditors and members of the public about insolvency proceedings; in particular, in their reports to creditors on debtor's affairs. Increasingly, insolvency practitioners are using web-based processes for this notification. A significant amount of information relating to insolvencies also is available on public registers, such as the National Personal Insolvency Index (NPII) database. The IPAA commented that the *Privacy Act* is hindering practitioners' roles in making available this information.[106]

44.83 In *Own Motion Investigation v Bankruptcy Trustee Firm*, the Privacy Commissioner considered the publication of bankruptcy information—including financial details—on an insolvency practitioner's website.[107] Some, but not all, of this information was publicly available from the bankrupt's Statement of Affairs and the NPII. The Commissioner accepted that the disclosure of a bankrupt's personal information to creditors for the purpose of administering the bankruptcy was permitted under the Act. She determined, however, that disclosure to parties who were not involved with the bankruptcy was a breach of the 'Use and Disclosure' principle. Publishing personal information on the internet without any limits on accessibility differs from accessing the information through publicly available sources. While an individual seeking access to the publicly available sources needs to make an application for a specific record and pay a fee, any internet user can browse hundreds of bankrupts' files. The Privacy Commissioner recommended that the insolvency practitioner should take steps to prevent general internet users from browsing the bankruptcy files, for example by securing the information using password protection.[108]

---

104 Ibid.
105 Ibid.
106 Ibid.
107 *Own Motion Investigation v Bankruptcy Trustee Firm* [2007] PrivCmrA 5.
108 Ibid.

ALRC's view

44.84 As a part of their functions, insolvency practitioners regularly handle, often sensitive, personal information. Their role includes collecting personal information through investigative processes and disclosing information to creditors and other interested parties. The ALRC does not, however, consider the *Privacy Act* to be unduly restricting this role.

44.85 Where inquiries or investigations made by an insolvency practitioner are specifically authorised under legislation, the disclosure of personal information by an agency or organisation will be permitted under the 'required or authorised by or under law' exception to the 'Use and Disclosure' principle.[109] This is rightly limited by the scope of the insolvency practitioner's statutory powers.[110] Where an agency or organisation is unclear whether a particular disclosure is within the purview of an insolvency practitioner's role, it is appropriate for them to request a more formal demand process.

44.86 There are clear policy reasons for insolvency proceedings to be made publicly available. This is reflected in the requirement that particulars of such proceedings be recorded on public registers. Insolvency practitioners' disclosure of personal information, however, is by no means unrestricted. In particular, care must be taken where personal information is made available on the internet.

44.87 In Chapter 11, the ALRC considers the tensions between public registers of information and individual privacy interests. Agencies and organisations are encouraged to restrict the type and extent of personal information that they publish on the internet. The ALRC also recommends that the OPC develop and publish guidance setting out factors that agencies and organisations should consider before publishing personal information in an electronic form.[111] This guidance will be relevant to insolvency practitioners that use web-based notification processes.

Valuers

44.88 Valuers assess the value of properties, including residential, commercial, industrial and retail properties. They may be engaged by private parties, corporations, financial institutions, or government departments and authorities. Private sector valuers

---

109 Currently, NPP 2.1(g) and IPPs 10.1(c) and 11.1(d) permit use or disclosure for a secondary purpose where this is 'required or authorised by or under law'. The ALRC is recommending that the model Unified Privacy Principles (UPPs) include an exception allowing an agency or organisation to use or disclose personal information where this is required or authorised by or under law. This will include use or disclosure to insolvency practitioners under the *Corporations Act* or *Bankruptcy Act*.

110 See *Complainant J v Statutory Entity* [2004] VPrivCmr 4. Disclosure of personal information to a court appointed liquidator turned on the correct legal interpretation of the scope of the liquidator's powers.

111 Rec 11–1.

are required to comply with the NPPs. Some state and territory legislation also regulates the handling of personal information by valuers.[112]

44.89 In its submissions to this Inquiry, the Real Estate Institute of Australia (REIA) proposed an exemption for valuers under the *Privacy Act*.[113] In its view, there is an overwhelming public need for accurate, up-to-date and reliable property information for the purposes of making appraisals and preparing valuation reports. It submitted that the ability of valuers to collect up-to-date and reliable personal and property information has been diminished by the *Privacy Act*.[114] The REIA stated that this

> lessens the quality and accuracy of their professional advice to financiers, businesses and consumers, which in turn places them at risk. These risks can be measured in terms of increased financial burdens, uncertainty in property values and investment potential, and flawed land tax and stamp duty assessments. Valuers will also be the subject of increasing litigation.[115]

44.90 There was little comment on this issue from other stakeholders. The ABA commented that 'a valuer is better able to determine whether a purchase has been the victim of a two tier marketing scheme or whether the transactions is at "arms length" for valuation purposes if the name and address of the purchaser is known'.[116] Other stakeholders submitted that they would oppose an exemption or exceptions for valuers.[117]

44.91 The REIA suggested that there already is sufficient protection for consumers under state legislation, such as the *Valuers Registration Act 1975* (NSW), to ensure that information in the hands of valuers is protected. [118]

ALRC's view

44.92 Individuals may reasonably expect that certain personal information collected by real estate agents in the course of selling a property—including the address of the property and the sale price—will be disclosed for valuation purposes. Individual

---

112 *Valuers Regulation 2005* (NSW) sch 2, r 9. *Valuation of Land Act 1916* (NSW) s 11 (for contract valuers engaged by state Valuers-General); *Valuation of Land Act 1978* (WA) ss 13, 14, 16; *Valuation of Land Act 2001* (Tas) ss 8, 53. For specialist retail valuers who are supplied information by landlords or tenants for the purposes determining the amount of rent under retail shop leases, see *Retail Leases Act 1994* (NSW) ss 19A(2), 31A(2); *Retail Leases Act 2003* (Vic) s 38; *Retail Shop Leases Act 1994* (Qld) s 35; *Business Tenancies (Fair Dealings) Act 2003* (NT) s 31.

113 Real Estate Institute of Australia, *Submission PR 400,* 7 December 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007; Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

114 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007; Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

115 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

116 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008.

117 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

118 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007; Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

vendors or purchasers, however, may not reasonably expect a real estate agent to disclose personal information, such as their names, to valuers.[119]

44.93 Assuming that the disclosure of the name of the vendor and purchaser (if individuals) would not reasonably be expected by them, the property industry could develop mechanisms to make known the relevant factors. This could involve, for example, a form that is filled out by an agent after a settlement is completed that sets out the principal characteristics of the sale, such as mortgagee sale, deceased estate, owner/occupier, investor, and so on.[120]

44.94 There is no compelling reason for an exemption or exception from *Privacy Act* obligations in relation to personal information disclosed to valuers by real estate agents, or more generally. There is adequate latitude for valuers to obtain information under the existing 'Use and Disclosure' principle and the model Unified Privacy Principles recommended in this Report. That is, disclosure is permitted for a related secondary purpose where the individual would reasonably expect such disclosure, or with the consent of the individual. Personal information required by valuers may also be obtained from land titles offices.

Archivists and archival organisations

44.95 Archivists and archival organisations are responsible for the collection, maintenance and management of records that are of enduring value and for making records available for access and research. Archival arrangements for public sector records are set out in Commonwealth and state and territory legislation and, consequently, are accommodated by exceptions in the *Privacy Act* for activities that are required or authorised by or under law. No equivalent provisions apply to private sector archival organisations.

44.96 In a submission to the Attorney-General's Department on the Privacy Amendment (Private Sector) Bill 2000 (Cth), the Australian Society of Archivists Inc and the Australian Council of Archives recommended an exemption for private sector archival organisations from the operation of the NPPs to facilitate research into the administrative, corporate, cultural and intellectual activity of Australia[121]—in particular, social and genealogical research.[122] In this Inquiry, one stakeholder submitted that 'complying with the NPPs is impossible if archives are to continue to

---

119 'Privacy Legislation and It's Effect on the Valuation Industry' (2003) *Australian Property Journal* 517, 518.

120 See Ibid.

121 Australian Society of Archivists Inc, *Submission to the Federal Privacy Commissioner on the Draft National Privacy Principle Guidelines*, 2 July 2001.

122 The special arrangements in place under the *Privacy Act 1988* (Cth) to allow for the use of personal information in health and medical research, and whether these arrangements should be extended to apply to research in areas such as criminology and sociology, is discussed in Chs 64, 65.

fulfil their valuable role in society and … information privacy should not last in perpetuity'.[123]

44.97 The ALRC did not receive submissions from archival organisations expressing concern about the impact of the *Privacy Act* on their activities.[124] The ALRC does not recommend any reform in relation to exempting or excepting archivists or archival organisations from obligations under the Act.

Declared emergencies

44.98 On 7 December 2006, a new Part VIA of the *Privacy Act* commenced operation.[125] Part VIA provides a separate regime for the collection, use and disclosure of personal information where there is a connection to an emergency that has been the subject of a declaration by the Prime Minister or a minister. The Part is intended to enhance information exchange between Australian Government agencies, state and territory authorities, organisations, non-government organisations and others, in emergencies and disasters.[126]

44.99 Part VIA arose partly as a response to the concern that the provisions of the *Privacy Act* impeded the ability of agencies and organisations to respond to the emergencies of the terrorist attacks in the United States on 11 September 2001, the Bali bombings of 2002 and the Boxing Day tsunami of 2004.

44.100 In summary, Part VIA operates as follows:

- The application of Part VIA is triggered by the making of a declaration by the Prime Minister or the relevant minister, where he or she is satisfied of a number of matters, including that there has been an emergency or disaster affecting one or more Australian citizens or permanent residents.[127]

- The declaration commences when it is signed and ceases to have effect at a specified time, when revoked or after a maximum of 12 months.[128]

---

123 Confidential, *Submission PR 134*, 19 January 2007.

124 The Australian Society of Archivists, the professional association for archivists and record-keeping professionals, made a submission on DP 72 advising of the need for good records management practices for privacy to be upheld. It did not suggest there was a need for archivists to have an exemption from the *Privacy Act* or an exception from particular privacy principles. Australian Society of Archivists, *Submission PR 460*, 11 December 2007.

125 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).

126 See *Privacy Act 1988* (Cth) s 80F; Explanatory Memorandum, Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Cth).

127 See *Privacy Act 1988* (Cth) ss 80J, 80K, 80L.

128 Ibid ss 80M, 80N.

- While such a declaration is in force, s 80P provides that an entity (which is defined to mean an agency, organisation or other person) may, for a 'permitted purpose',[129] collect, use or disclose personal information relating to an individual if: the entity reasonably believes the individual may be involved in the emergency or disaster; and the disclosure is to one of the persons specified.

- Section 80Q creates an offence to disclose information obtained under Part VIA in certain circumstances, punishable by a penalty of 60 penalty units[130] and/or imprisonment for one year.

- Division 4 of Part VIA also contains a number of technical provisions including a severability provision and a provision dealing with compensation.

44.101 Before the *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth) was passed, a number of stakeholders informed the ALRC that the *Privacy Act* hinders operations in emergency situations. Following the introduction of the amendment, however, a number of stakeholders have indicated that most, if not all, of the problems arising from the handling of personal information in emergency situations have been dealt with adequately by the advent of Part VIA.[131]

44.102 In the ALRC's view, it would be premature to propose changes to the regime before there has been any opportunity to evaluate how well the provisions operate in practice.

---

129 The term 'permitted purpose' is defined in s 80H and includes: identifying injured, missing, dead or affected individuals; assisting affected individuals in accessing services; and assisting law enforcement and coordinating the management of the situation.

130 Currently this amounts to $6,600.

131 See, eg, Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Australian Taxation Office, *Submission PR 168*, 15 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.

Part F

Office of the Privacy Commissioner

45. Overview: Office of the Privacy Commissioner

Contents

Introduction

45.1 Part F is concerned with the Office of the Privacy Commissioner (OPC). The OPC is an independent statutory body established by the *Privacy Act 1988* (Cth), consisting of the Privacy Commissioner and staff appointed under the Act. The OPC is responsible for administering the *Privacy Act*, and is the federal regulator for privacy in Australia.

45.2 General privacy regulation has operated at a federal level only since the *Privacy Act* was passed in 1988. In the early years of privacy regulation, the Privacy Commissioner was responsible for overseeing compliance with the Act by agencies

and tax file number recipients. Since that time, however, the responsibilities of the OPC have widened significantly to include credit providers, credit reporting agencies and the private sector. These changes resulted in more functions and powers for the Commissioner, although not always a commensurate increase in resources.

45.3 This chapter sets out the key themes arising out of Part F, and summarises some of the major reforms recommended by the ALRC. The chapter also examines the ALRC's approach to addressing systemic issues in privacy compliance. Before turning to those matters, however, the chapter considers the consolidation of the Commissioner's functions.

Consolidating functions

45.4 The *Privacy Act* divides the Privacy Commissioner's functions between interferences with privacy generally, tax file numbers and credit reporting. This division is a product of the historical development of the *Privacy Act*. Consistently with the ALRC's recommendation that the *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity,[1] it would add greater clarity to the Act to consolidate the functions of the Commissioner where appropriate.

45.5 For example, the Privacy Commissioner's functions to investigate potential breaches of the Information Privacy Principles (IPPs), National Privacy Principles (NPPs), Tax File Number Guidelines[2] and credit reporting provisions, should be consolidated into a general function to investigate 'interferences with privacy'. This term 'interference with privacy' is already defined to include breaches of these respective provisions. The specific functions in ss 28(1)(b)–(c) and 28A(1)(b) should then be repealed. This consolidation is particularly important if and when the ALRC's model Unified Privacy Principles (UPPs) are adopted.

45.6 Similarly, the credit reporting guidelines, advice and education functions in s 28A[3] could be rolled into their equivalent functions in s 27[4] or moved to the new *Privacy (Credit Reporting Information) Regulations*.[5]

Facilitating compliance with the *Privacy Act*

Compliance-oriented regulation

45.7 As examined in Chapter 4, the *Privacy Act* is a principles-based regime. As such, it relies on relatively high-level principles to set out the objects that Parliament has determined regulated entities should achieve in dealing with personal information. These objects are, for example: to collect only information that is necessary to fulfil the

---

1 Rec 5–2.
2 To be renamed *Tax File Number Rules*: see Rec 47–2(a).
3 Respectively s 28A(1)(e), (f), and (k).
4 Those functions are *Privacy Act 1988* (Cth) s 27(1)(e), (f), and (m) respectively.
5 See Part G.

regulated entity's functions; to take reasonable steps to secure data; and to take reasonable steps to ensure that the data is accurate.

45.8 In a principles-based regime, the regulator plays a particularly significant role, for a number of reasons. First, in supporting the continuation of principles-based regulation for the privacy regime in Australia, the ALRC is supporting both the use of principles as the primary regulatory tool and also the adoption of a more outcomes-based approach to regulating privacy.[6] In particular, the ALRC endorses the emphasis on fostering and securing compliance through guidance, education and other facilitative methods.

45.9 The emphasis on guidance raises the second reason why a regulator plays a pivotal role in a principles-based regime. Guidance is a critical part of administering a principles-based regime such as the *Privacy Act* and, as such, is a key component of the ALRC's recommended regulatory model. The OPC must play a critical role in providing this guidance, to help regulated entities understand their obligations under the *Privacy Act*. Throughout this Report, the ALRC has made recommendations to increase the level of guidance offered by the OPC.

45.10 The other key components of the regulator's role in a compliance-oriented regulatory design is to monitor compliance and enforcement. While Chapter 4 explores the theory behind these issues in more detail, Part F looks at the functions and powers of the federal privacy regulator which will help give life to the ALRC's model of compliance-oriented regulation. In particular, it is useful to consider the powers set out in Chapter 47 in terms of their purpose in either fostering compliance (for example, the oversight powers) and monitoring compliance (such as the audit powers), and the powers in Chapters 49 and 50 in relation to enforcing compliance.

Structure of the OPC

Regulatory structure

45.11 Chapter 46 sets out the ALRC's recommended regulatory structure for the OPC. The chapter provides an overview of the Privacy Commissioner's powers and examines the accountability mechanisms to which the Commissioner is subject under the *Privacy Act*. The ALRC recommends that the name of the OPC should be changed to the 'Australian Privacy Commission' and that the number of statutory appointees should be increased.[7] The ALRC also recommends that the matters the Commissioner must have regard to in exercising his or her powers should be aligned with the

6 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 3.

7 Recs 46–1, 46–2.

recommended objects of the *Privacy Act*.[8] Finally, the chapter examines the assistance given to the OPC by the Privacy Advisory Committee and recommends reform to the composition of the Committee.[9]

Powers of the OPC

45.12 Chapter 47 examines the functions and powers vested in the Privacy Commissioner by the *Privacy Act*. The general approach of the *Privacy Act* is to state the Commissioner's 'functions' and give the Commissioner 'power' to do all things necessary or convenient to be done for or in connection with the performance of his or her functions. While much of this Report refers to the 'OPC', the actual functions and powers outlined in the *Privacy Act* are vested in the Privacy Commissioner and are to be exercised—or delegated—by the individual appointed as Privacy Commissioner.

45.13 The Privacy Commissioner has functions in relation to interferences with privacy generally, tax file numbers and credit reporting. The Commissioner also has compliance functions under other federal legislation.

Oversight and compliance functions

45.14 Chapter 47 considers the Privacy Commissioner's functions of overseeing and monitoring compliance with the *Privacy Act*—including the functions of giving advice and guidance, undertaking educational programs, and conducting audits—and the Commissioner's powers to issue Public Interest Determinations. The ALRC makes a number of recommendations to reform these functions, to expand and strengthen the Commissioner's powers of securing and monitoring compliance with the *Privacy Act*. One recommendation is to empower the Privacy Commissioner to conduct a Privacy Performance Assessment of an organisation's compliance with the model UPPs, privacy regulations, rules and any privacy code that binds the organisation.[10]

Privacy impact assessments

45.15 Chapter 47 also examines the very topical issue of Privacy Impact Assessments. The chapter looks at the role of Privacy Impact Assessments in the regulatory regime, and considers the role they play in facilitating privacy compliance. The ALRC recommends that the *Privacy Act* should be amended to empower the Privacy Commissioner to direct an agency to provide to the Commissioner a Privacy Impact Assessment in relation to a new project or development that the Commissioner considers may have a significant impact on the handling of personal information.[11] Another recommendation is that guidelines be developed for organisations to

8 Rec 46–3.
9 Rec 46–4.
10 Rec 47–6.
11 Rec 47–4.

encourage them to use Privacy Impact Assessments as part of their planning processes.[12]

Privacy codes

45.16 The ALRC considers the co-regulatory aspects of the *Privacy Act* in Chapter 48. These are the provisions in Part IIIAA that allow organisations to develop privacy codes, which, when approved by the OPC, replace the NPPs. The ALRC recommends that the provisions be amended so that privacy codes do not replace the model UPPs, but operate in addition to them, providing guidance on how one or more of the principles are to be applied or complied with by an agency or organisation.[13]

Investigation and resolution of privacy complaints

45.17 Concern has been expressed by stakeholders about the current complaint-handling process in the *Privacy Act*. In Chapter 49, the ALRC makes recommendations to reform the existing provisions to streamline, and increase the effectiveness of, complaint handling under the Act.

Addressing systemic issues

45.18 Stakeholders in this Inquiry and previous inquiries conducted on aspects of the *Privacy Act*, have consistently expressed concern about the ability of the OPC to address systemic issues in privacy compliance. By systemic issues, the ALRC is referring to 'issues that are about an organisation's or industry's practice rather than about an isolated incident'.[14]

45.19 To facilitate a shift in focus to systemic issues, the ALRC has made a number of recommendations that would permit the OPC to devolve some of the responsibility for handling privacy complaints under the Act. Some privacy complaints, particularly in the credit reporting area, could be handled by external dispute resolution schemes. The ALRC recommends that the Privacy Commissioner be given a specific decline and referral power for these purposes.[15]

45.20 The ALRC also recommends that the Privacy Commissioner's power to remedy systemic issues be enhanced by empowering the Commissioner to prescribe, in a determination, the steps an agency or organisation must take to comply with the *Privacy Act*.[16]

---

12 Rec 47–5.
13 Rec 47–6.
14 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 130 fn 102.
15 Rec 49–2.
16 Rec 49–6.

Framework for conciliation and determination

45.21 The second central issue examined in Chapter 49 is the manner in which complaints are resolved under the *Privacy Act*. The ALRC recommends that the Act be amended to include a new framework to deal with conciliation and determination. This framework would, among other things, give complainants and respondents the right, in certain circumstances, to require the Commissioner to resolve a complaint by determination.[17]

Accountability and transparency

45.22 Chapter 49 also considers issues of accountability and transparency in handling privacy complaints. The ALRC recommends that the *Privacy Act* be amended to provide merits review of all determinations made by the Privacy Commissioner and that the OPC publish a document setting out its complaint-handling policies and procedures.[18]

Enforcing the *Privacy Act*

Own motion investigations

45.23 Chapter 50 examines the Privacy Commissioner's powers to enforce compliance with the *Privacy Act*. The chapter focuses on the Privacy Commissioner's powers to commence, on the Commissioner's own motion, an investigation into an act or practice that may be an interference with privacy. This own motion investigation power complements the Commissioner's power under the *Privacy Act* to investigate complaints. A significant limitation on the Commissioner's own motion investigation power, however, is the inability to prescribe or enforce remedies where the Commissioner finds that an agency or organisation has contravened the privacy principles. The ALRC recommends that the Privacy Commissioner be empowered to impose remedies where he or she finds a breach of the principles following an own motion investigation.[19]

Strengthening the enforcement pyramid

45.24 Chapter 50 also considers the question whether there needs to be further remedies or penalties available under the Act to enforce compliance. Taking into account the enforcement pyramid approach discussed in Chapter 4, the ALRC recommends that civil penalties be introduced for serious or repeated interferences with the privacy of an individual.[20] This recommendation is intended to strengthen the overall enforcement pyramid underpinning the *Privacy Act*, and should provide strong incentives for increased compliance by agencies and organisations.

---

17 Rec 49–5.
18 Rec 49–7, 49–8.
19 Rec 50–1.
20 Rec 50–2.

Enforcement approach

45.25 It is crucial that there be an element of public enforcement in the OPC's regulation of privacy, consistent with Parliament's expectation that the Commissioner 'be the means by which there will be accountability to the public on the use by government of their personal information'.[21] This expectation applies equally to the use of personal information by organisations.

45.26 A clear enforcement policy that outlines what the OPC's usual response to a particular type of breach will be and how that response can be addressed—such as by evidence of a good internal compliance program—can provide incentives for agencies and organisations to put in place those mitigating practices. Such a policy also allows the regulator to discriminate between agencies and organisations that are genuinely trying to comply and those that are not. The regulator can then adopt enforcement responses that send a strong message of general deterrence to the regulated community. This will or is likely to encourage agencies and organisations to keep complying (or at least keep trying to comply), as they will realise that non-compliance, combined with no effort to comply, will attract strong sanctions from the regulator.

45.27 Consistent with the compliance-oriented regulatory design underpinning the *Privacy Act*, the OPC should implement a compliance policy that adopts an explicit enforcement pyramid approach to restoring compliance with, and enforcing, the *Privacy Act*. The OPC should use, and should be seen to be using, a wide range of strategies to ensure compliance with the *Privacy Act*, recognising the benefits of specific and general deterrence that can be generated by a transparent, balanced and vigorous enforcement approach.

Data breach notification

45.28 Chapter 51 examines data breach notification. The security of personal information is a growing concern in privacy regulation around the world. One regulatory response to the increasing number of data breaches has been to require agencies or organisations to notify individuals affected where there has been an unauthorised acquisition of personal information.

45.29 In Chapter 51, the ALRC considers the rationale behind mandatory reporting of data breaches, and examines some of the models for data breach notification laws. The key issues considered are the triggering event, the general exceptions to notification and the scope of the responsibility to notify.

---

21 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General). This speech only refers to the government, as organisations were not covered by the *Privacy Act* when the Act was originally passed.

New data breach notification provisions

45.30 There is a strong regulatory justification for introducing a requirement for agencies and organisations to report data breaches to individuals affected and to the OPC. The ALRC recommends a model where notification would be required if 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. In determining whether there is a real risk of serious harm, consideration should be given to whether the information was encrypted adequately and whether the breach was internal and there was no further disclosure. Notification is not required where the Privacy Commissioner does not consider that it would be in the public interest. To provide strong incentives for compliance with the data breach notification provisions, the ALRC recommends that failure to notify the Commissioner of a data breach attract a civil penalty.[22]

Summary of recommendations to address systemic issues

45.31 As noted above, a major concern of stakeholders is the limited ability of the OPC to address systemic issues. The OPC requires a number of tools and strategies to enable it to discover, monitor and remedy systemic issues in agencies, organisations and industries. Ideally, these tools and strategies must allow the Privacy Commissioner to act proactively to identify and resolve systemic issues before a breach occurs and, when enforcing the Act, to act in a manner that deters the agency or organisation involved and acts as a general deterrent to other agencies and organisations.

45.32 The ALRC makes a number of recommendations throughout Part F that are aimed at increasing the OPC's ability to monitor and remedy systemic issues. Taken as a whole, these recommendations would provide the OPC with an appropriate 'toolkit' to deal with systemic issues in privacy compliance.[23]

Resources

45.33 As noted above, since the commencement of the *Privacy Act*, the responsibilities of the OPC have widened significantly, with more functions and powers being vested in the Commissioner. These changes have not always been accompanied by a commensurate increase in resources.

45.34 A key theme in this Inquiry has been a lack of confidence among stakeholders in OPC as both the industry regulator and the complaint-handling body for privacy complaints (including credit reporting). For example, stakeholders expressed the view

22 Rec 51–1.
23 See, eg, Recs 47–6, 49–5, 49–6, 50–1, 50–2.

that the OPC has taken too long to resolve complaints and dismissed complaints too readily.[24] One stakeholder argued:

> With limited resources, there is always a tension between undertaking individual complaints handling and working to address broader, systemic issues. Neither function, however, should be ignored.[25]

45.35 Many of these problems can be attributed to the increase in the OPC's functions with the addition of the responsibilities for the private sector in 2001 without a corresponding increase in budget. In 2006, the OPC's budget was enhanced, which has allowed it to devote resources to clearing the backlog of complaints and shift its focus towards other areas of responsibility.

45.36 The recommendations contained in this part of the Report, and the ALRC's other recommendations for greater clarity, guidance and new responsibilities under the *Privacy Act*[26] will have significant resource implications for the OPC. It is critical that the OPC remain adequately resourced so that it is able to implement recommended initiatives and retain the trust of the entities subject to the *Privacy Act* and the community at large. Without adequate resourcing, the beneficial outcomes that will flow from the implementation of the ALRC's recommendations will not be realised.

---

24 See Ch 49.

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

26 See, eg, Recs 6–2, 10–3, 16–2, 19–1, 21–2, 23–3, 40–2, 56–7, 60–3, 67–2, 74–7.

46. Structure of the Office of the Privacy Commissioner

Contents

Introduction

46.1 This chapter considers the structure of the Office of the Privacy Commissioner (OPC). The discussion focuses on the existing structure, functions and powers of the Privacy Commissioner, the constraints on the exercise of the Commissioner's powers, the liabilities to which the Commissioner is subject and the immunities the Commissioner enjoys. The chapter also considers the Privacy Advisory Committee, including its composition and functions.

Structure, functions and powers

Legislative structure

46.2 The role and position of Privacy Commissioner was originally established in the *Privacy Act 1988* (Cth). The Commissioner was initially a member of the Human Rights and Equal Opportunity Commission (HREOC), before the OPC was established as a separate office in July 2000. It was suggested that a separate office was consistent with the approach taken in other countries and that it would provide 'an opportunity to further increase the profile, and thus the effectiveness, of the work of the Privacy Commissioner and of the office of the Privacy Commissioner'.[1]

46.3 The *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* (Cth) amended the *Privacy Act* to establish the 'Office of the Privacy Commissioner', defined to consist of the Privacy Commissioner and staff appointed under s 26A.[2] The *Privacy Act* provides that the Commissioner is appointed by the Governor-General for a period of up to seven years,[3] on such terms and conditions as imposed by the Governor-General and the Act.[4] The Commissioner's appointment may be terminated because of misbehaviour, or physical or mental incapacity, and must be terminated in circumstances of bankruptcy, extended absence or unapproved outside employment.[5]

46.4 The *Privacy Act* does not provide for a Deputy or Assistant Commissioner (as a statutory appointee), but does provide for the appointment of an Acting Commissioner during any vacancy in the office or absence of the Privacy Commissioner.[6] Although this is similar to the approach taken in Australian states, both Canada and New Zealand provide for the appointment of additional statutory officers.

46.5 For instance, in New Zealand, the Governor-General may, on the recommendation of the Minister, appoint a Deputy Commissioner, who is entitled to all the protections, privileges and immunities of the Commissioner and, subject to the

---

1 Commonwealth, *Parliamentary Debates*, House of Representatives, 9 December 1998, 1660 (D Williams—Attorney-General), 1660.
2 *Privacy Act 1988* (Cth) s 19.
3 Ibid ss 19A(1), 20(1).
4 Ibid s 20.
5 Ibid s 25.
6 Ibid s 26.

control of the Commissioner, has and may exercise all the powers, duties and functions of the Commissioner under the Act.[7] In Canada, the Governor in Council may, on the recommendation of the Privacy Commissioner, appoint one or more Assistant Privacy Commissioners. The Assistant Privacy Commissioners hold office during good behaviour for a term not exceeding five years and are to engage exclusively in such duties or functions of the office of the Privacy Commissioner under the *Privacy Act* or any other Act as are delegated by the Privacy Commissioner to the Assistant Privacy Commissioner.[8]

Functions and powers of the OPC

46.6 Part IV, Division 2 of the *Privacy Act* vests a range of functions in the Commissioner. These functions are examined in Chapters 47–49 and are divided in the Act into functions relating to interferences with privacy, tax file numbers and credit reporting.[9] The Privacy Commissioner also has functions under other Acts, which are examined further in Chapter 47 and Part J.

46.7 The *Privacy Act* invests the Commissioner with power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions.[10] The Commissioner also has an ancillary function in s 27(1)(s) to do anything incidental or conducive to the performance of any of the Commissioner's other functions in s 27(1).[11]

Delegation

46.8 There are two matters to note about the Commissioner's legislative functions and powers. The first is that the *Privacy Act* invests functions in the Privacy Commissioner personally, rather than in the OPC generally, and only the Commissioner has the power to do all things necessary or convenient to be done in connection with the performance of his or her functions.

46.9 Secondly, the Privacy Commissioner can delegate all or any of his or her powers either to a member of the Commissioner's staff or a member of the staff of the Commonwealth Ombudsman, with two exceptions. The Commissioner cannot delegate the powers conferred by s 52, which sets out the Commissioner's power to make

---

7 *Privacy Act 1993* (NZ) s 15.

8 *Privacy Act* RS 1985, c P-21 (Canada) ss 56–57.

9 The Commissioner's functions and powers in relation to general interferences with privacy are set out in detail in Ch 47. The Commissioner's functions in relation to credit reporting are discussed in Part G.

10 *Privacy Act 1988* (Cth) ss 27(2), 28(2), 28A(2).

11 Ibid s 34 limits the Commissioner's powers 'in connection with the performance of the functions referred to in section 27' in relation to documents exempt under the *Freedom of Information Act 1982* (Cth).

determinations, and the Commissioner cannot delegate his or her power under s 17 to issue guidelines relating to tax file number information.[12]

Regulatory structure

46.10 The Privacy Commissioner, supported by the OPC, is an individual, independent regulator, rather than a regulatory agency or commission.[13] There has been some discussion by regulatory theorists about the distinction between an independent individual regulator, such as the Privacy Commissioner, and a commission-style regulator. It has been noted that the rationale for attaching regulatory powers to an individual is

> 'to seek to develop a quicker and less bureaucratic system of regulation. This was centred on the idea of a single, independent regulator for each industry, operating without undue bureaucracy and supported by a small staff.' It was considered, further, that personal responsibility for regulation would reassure the public who could identify regulation with an individual protector of their interests rather than some vague commission of faceless persons.[14]

46.11 The disadvantages of an individual regulator include: the possibility that significant political pressures may be directed at one person; a lack of accountability to a board or equivalent; and the potential for unpredictable decision making.[15] An individual regulator structure means 'important decision making functions which are material to the rights and privileges of third parties' are vested in one individual, which could result in one individual being responsible for advising organisations and adjudicating disputes involving the same organisation.[16] This can raise the danger that the regulator will, or will be seen to, 'fall between stools' such that its enforcement actions are seen as tainted by its policy-making concerns, and vice versa.[17]

46.12 An alternative structure to an individual regulator is a commission. Proponents of commissions argue that a commission structure: helps reduce the danger that regulators will feel vulnerable and behave defensively; creates a sense that decisions follow internal debate; increases legitimacy and accountability; and spreads the workload involved in regulating complex industries.[18] Critics, however, argue that a commission structure may lead to: inconsistent decisions, as decisions would be made

---

12 *Privacy Act 1988* (Cth) s 99.

13 Note that s 26A of the *Privacy Act* provides that the Commissioner and the Australian Public Service employees assisting the Commissioner constitute a Statutory Agency for the purposes of the *Public Service Act 1999* (Cth) and the Commissioner is the Head of the Statutory Agency.

14 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 71: quoted in United Kingdom Government National Audit Office, *The Work of the Directors General of Telecommunication, Gas Supply, Water Services and Electricity Supply* (2006), [2.3].

15 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 324.

16 United Kingdom Director General of Telecommunications, *Submission to the Review of Utility Regulation*, 1 September 1997, [5.31].

17 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 70–71.

18 Ibid, 324.

by a commission whose composition may change; slower decision making; and possible loss of clarity of responsibility.[19]

Submissions and consultations

46.13 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC identified support in submissions and consultations for the current legislative structure of the OPC.[20] The OPC noted in particular that the OPC's structure as a statutory body with a Commissioner appointed for a specified term is consistent with international standards regarding privacy regulation.[21]

46.14 The OPC raised several issues, however, in relation to the OPC's legislative structure. First, the OPC noted that the delegation power prohibits the Commissioner from delegating the power under s 52 to make determinations (or as the power to issue tax file guidelines under s 17). In the OPC's view, this restriction meant the exercise of the determination power is necessarily limited to the individual Commissioner's availability, which, given the OPC's commitment to making more determinations, was problematic. Consequently, the OPC suggested that the *Privacy Act* be amended to allow the power in s 52 to be exercised by senior staff members (such as the Deputy or Assistant Privacy Commissioner).

46.15 Secondly, the OPC reiterated its recommendation that the name of the Office should be changed to the 'Australian Privacy Commission'.[22] The OPC argued that the similarity of names between state privacy regulators and the OPC causes confusion for consumers who are trying to work out to whom they should make a complaint. The OPC also argued that renaming the office as suggested would be more consistent with other federal regulators, such as the 'Australian Competition and Consumer Commission' and the 'Australian Securities and Investments Commission'.[23]

Discussion Paper proposals

46.16 In DP 72, the ALRC made a number of proposals to amend the legislative structure of the OPC. The ALRC supports the independent nature of the OPC and

---

19 Ibid, 324–325.

20 See 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; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

21 See *Criteria and Rules for Credentials Committee and the Accreditation Principles*, (Adopted on 25 September 2001 during the 23rd International Conference of Data Protection Commissioners held in Paris, 24–26 September 2001 and as amended on 9 September 2002 during the 24th International Conference of Data Protection and Privacy Commissioners held in Cardiff 9–11 September 2002).

22 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 6.

23 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 47.

proposed that the number of statutory officers at the OPC be extended to include one or more Deputy Privacy Commissioners, who, subject to the Privacy Commissioner's oversight, could exercise all the functions conferred on the Privacy Commissioner.[24] In the ALRC's view, this would enable more than one person to exercise important functions such as the determination power in s 52 of the *Privacy Act*, and would also facilitate an expansion of the OPC to a commission-style body.

46.17 The move to a commission-style body was also supported by the proposal to change the OPC's name to the 'Australian Privacy Commission'.[25]

Submissions and consultations on DP 72

46.18 The ALRC received a number of submissions on both of these proposals. In relation to the proposed name change, all stakeholders that commented on the proposal were in support of changing the OPC's name to the 'Australian Privacy Commission'.[26] The inclusion of 'Australian' in the name change was thought to be more consistent with other federal regulators and 'is a more appropriate name for the office to have in the context of its function of engaging in the international privacy arena'.[27] The change of name was also thought to reflect the expansion of the OPC's functions and purview.[28]

46.19 Support was also expressed by several stakeholders for the ALRC's proposal to allow for the appointment of Deputy Privacy Commissioners as statutory officers.[29] The Law Society of New South Wales commented that '[a]n effective infrastructure for

---

24 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 43–2.

25 See Ibid, Proposal 43–1.

26 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; GE Money Australia, *Submission PR 537*, 21 December 2007; Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Centre for Law and Genetics, *Submission PR 497*, 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 Health and Medical Research Council, *Submission PR 397*, 7 December 2007. The Australian Direct Marketing Association 'does not disagree' with this proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

27 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

28 See Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007.

29 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 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 Health and Medical Research Council, *Submission PR 397*, 7 December 2007. The Australian Direct Marketing Association 'did not disagree' with this proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

the regulation of privacy matters needs a properly structured and constituted responsible body to promote the legislative purposes of the *Privacy Act* and to protect the privacy of individuals'.[30]

46.20 The Public Interest Advocacy Centre (PIAC) welcomed the ability of the Deputy Commissioners to exercise the determinations function, describing the exercise of the determinations power as 'fundamental to the effective operation of the Act'. PIAC also noted that 'multiple statutory officers will allow for greater separation of the functions of the Office, thus avoiding perceived conflicts between these functions'.[31] The Australian Privacy Foundation supported, in principle, the expansion of the OPC to include at least two statutory officers but expressed concern that the relationship between the Deputy Privacy Commissioner and the Privacy Commissioner required further clarification.[32]

46.21 In contrast, the OPC strongly opposed the appointment of further statutory officers to the OPC. While agreeing that officers in addition to the Commissioner should have the ability to exercise all of the powers, duties and functions of the Privacy Commissioner, including those conferred by ss 52 and 28(1)(a), the OPC did not believe it was necessary that such officers be statutorily appointed in order to exercise effectively those powers, duties and functions. In relation to the ALRC's suggestion that the significance of the determinations power is such that it should be exercised only by independent, statutory officers, the OPC submitted:

> The exercise of the determination power in s 52 is significant, however its proper use is not impacted by the method by which an officer was appointed, but rather by the capacity of that officer to exercise the power in accordance with principles of administrative law. This Office does not consider that the statutory appointment of one or more Deputy Commissioners is necessary for the independent, transparent and accountable exercise of those powers.[33]

46.22 The OPC submitted that, consistently with the CEO responsibilities of the Commissioner, 'it is more appropriate that the Commissioner appoint and manage senior staff'.[34]

Office of the Information Commissioner

46.23 During the 2007 federal election, the Australian Labor Party proposed bringing together the functions of privacy protection and freedom of information in an 'Office of the Information Commissioner'. This office would preserve the existing role of the

---

30 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

31 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

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

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

34 Ibid.

Privacy Commissioner and appoint a Freedom of Information Commissioner as a statutory office holder responsible for freedom of information law.[35] At the time this Inquiry was completed, this policy had not yet been implemented.

46.24 Smartnet expressed a preference for a combined office of Information Commissioner and Privacy Commissioner, as proposed by the Australian Labor Party. Smartnet suggested that by creating a combined Office of Information Commissioner, the government has the 'opportunity to coherently and consistently deal with both privacy and data protection'.[36]

46.25 Following the release of DP 72, on 24 September 2007, the former Attorney-General of Australia referred to the ALRC for inquiry and report matters relating to the extent to which the *Freedom of Information Act 1982* (Cth) and related laws continue to provide an effective framework for access to information in Australia.[37] Some of the interaction between privacy and freedom of information laws may be considered by this inquiry, including the location of an office holder with responsibility for freedom of information law.[38]

ALRC's view

46.26 The legislative structure of the OPC is an integral part of building an effective infrastructure for privacy regulation in Australia. It is critical that the body responsible for regulating the personal information-handling practices of the federal public sector and applicable organisations is named, structured and constituted in a manner that best helps it achieve its legislative purpose to promote and protect privacy in Australia.[39]

46.27 The approach of compliance-oriented regulation adopted by the ALRC in its regulatory model requires the Commissioner to play a pivotal role in securing the compliance of regulated entities with the *Privacy Act*, monitoring that compliance, and enforcing compliance. While the remit of the *Privacy Act* is already very wide, the ALRC makes several recommendations in this Report which will widen it further. These include the recommendation to remove the small business exemption and for further expansion and exercise of the OPC's powers to enable it to monitor and enforce compliance more effectively.[40] These recommendations are likely to increase significantly the workload of the OPC. It is important to consider, therefore, whether the current legislative structure of the OPC is adequate to fulfil these roles and meet the needs of the community.

---

35 K Rudd and J Ludwig, *Government Information: Restoring Trust and Integrity—Election 2007 Policy Document* (2007) Australian Labor. This proposal is discussed further in Ch 15.

36 Smartnet, *Submission PR 457*, 11 December 2007.

37 The Terms of Reference are available on the ALRC website at <www.alrc.gov.au/inquiries/current/foi/terms.htm>.

38 This issue is discussed further in Ch 15.

39 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 14 April 2008.

40 Rec 39–1.

46.28 The OPC should be renamed the 'Australian Privacy Commission' and the *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. These Deputy Privacy Commissioners would be able to exercise all the powers, duties and functions of the Privacy Commissioner under the *Privacy Act*—including a power conferred by s 52 and a power in connection with the performance of the function of the Privacy Commissioner set out in s 28(1)(a)—or any other enactment.

46.29 Privacy is a growing international and local issue, manifested in many different areas, including cross-border information flows, the internet, e-commerce and e-health issues. The international dimension of privacy regulation requires a well-resourced and prominent regulator to contribute and influence the development of international regulatory relationships and responses to emerging issues. Providing for the appointment of one or more Deputy Privacy Commissioners, as statutory office holders with the attendant rights and protections, is an important step to expand the size of the federal privacy regulator, and should encourage a commensurate increase in the perception of the importance of the privacy regulator and privacy regulation in Australia.

46.30 This recommendation to appoint further statutory officers would facilitate a move to a commission-style body, which would have a flatter distribution of responsibility across a number of individuals. This is consistent with the renaming of the OPC to the 'Australian Privacy Commission'.

46.31 Increasing the number of statutory officer holders also allows for greater collegiate decision making, encouraging greater accountability and transparency in operations, but still ensuring there is a 'head' governing the body as a whole. If the Privacy Commissioner desired, the office could be divided formally into Divisions, with a Deputy Commissioner heading each division and with the Privacy Commissioner continuing to oversee the entire operation of the Commission. As noted by some stakeholders, this would help avoid perceived conflicts between the different arms of the office.[41]

46.32 Importantly, the ALRC's recommended legislative structure retains the benefits of having a visible and prominent 'head' of the organisation, as the Privacy Commissioner would remain paramount given the oversight role of the Commissioner. The ALRC notes that there have been several Deputy Privacy Commissioners

41 See Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

appointed in Canada, to guarantee 'ethical decision-making and values-based management'.[42]

46.33 Increasing the number of statutory appointees would provide a means to address the delegation issue raised by the OPC in its submission to the Issues Paper, *Review of Privacy* (IP 31). The Act currently prohibits the Privacy Commissioner from delegating his or her power to make determinations under s 52 (as well as the power to issue tax file number guidelines under s 17). In the ALRC's view, the determination power is significant and should be exercised only by statutory officers appointed under *Privacy Act*. Although—following the High Court's decision in *Brandy v Human Rights and Equal Opportunity Commission*[43]—determinations are no longer binding and conclusive between parties, the power to issue determinations is still one of the most significant powers vested in the Commissioner.

46.34 The recommendation to appoint more statutory officers who are expressly authorised to exercise all the powers of the Privacy Commissioner—including a power under s 52—respects the significance of the power in s 52 and ameliorates the problem of it being limited to one person's availability. Having additional statutory officers with power to make determinations should also give the OPC the means to address concerns about the rare use of the determinations power. It would also facilitate implementation of the ALRC's recommendation to give complainants and respondents the right, in certain circumstances, to require the Commissioner to issue a determination in relation to their complaint.[44]

46.35 The ability to appoint more than one statutory officer would enable the OPC to develop strong expertise in emerging areas of regulation. For example, a Shared National Electronic Health Record system[45] could require the OPC to allocate significant resources towards its oversight. In such circumstances, it may be useful to appoint a Deputy Commissioner with health privacy expertise to head a health privacy division in the OPC.

---

42 Office of the Privacy Commissioner of Canada, 'Interim Privacy Commissioner Responds to OAG and PSC Audits' (Press Release, 30 September 2003).

43 *Brandy v Human Rights and Equal Opportunity Commission* (1995) 183 CLR 245. Following *Brandy*, the *Human Rights Legislation Amendment Act 1995* (Cth) removed the Commissioner's power to register determinations in the Federal Court.

44 Rec 49–5.

45 See Ch 61.

Recommendation 46–1 The *Privacy Act* should be amended to change the name of the 'Office of the Privacy Commissioner' to the 'Australian Privacy Commission'.

Recommendation 46–2 The *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. The Act should provide that, subject to the oversight of the Privacy Commissioner, the Deputy Commissioners may exercise all the powers, duties and functions of the Privacy Commissioner under the Act or any other enactment.

Manner of exercise of powers

Section 29 of the *Privacy Act*

46.36 In exercising his or her powers under the *Privacy Act*, the Commissioner is bound to have regard to the matters set out in s 29. The matters in s 29 can be divided into two principal concerns. First, the *Privacy Act* requires the Commissioner to take the following into account when performing functions and exercising a power:

- protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the recognition of the right of government and business to achieve their objectives in an efficient way;[46] and

- international obligations accepted by Australia, including those concerning the international technology of communications, and developing general international guidelines relevant to the better protection of individual privacy.[47]

46.37 Secondly, the *Privacy Act* requires the Commissioner to ensure that his or her recommendations, directions and guidelines are capable of being accepted, adapted and extended throughout Australia,[48] and are consistent with whichever is relevant out of the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs), the *Credit Reporting Code of Conduct* and Part IIIA of the Act.[49]

46.38 The Explanatory Memorandum to the Privacy Bill 1988 (Cth) explained that s 29 requires the Commissioner 'to balance the need to ensure proper protection from

46 *Privacy Act 1988* (Cth) s 29(a).
47 Ibid s 29(b).
48 Ibid s 29(c).
49 Ibid s 29(d).

interferences of privacy against the requirements of government and private sector bodies to achieve their objectives in an efficient manner'.[50] The OPC has previously explained that 'the legislation acknowledges that privacy is not an absolute right and that an individual's right to protect his or her privacy must be balanced against a range of other community and business interests'.[51] Stakeholders to this Inquiry generally supported s 29 and the requirement that privacy be balanced against other community interests.[52]

46.39 The New Zealand *Privacy Act* requires its Privacy Commissioner to have regard to largely the same matters as set out in s 29.[53] In other jurisdictions, an alternative approach is taken. Instead of explicitly requiring privacy regulators to have regard to certain matters in the exercise of their powers, the privacy legislation acknowledges matters such as the competing interests of human rights and organisational efficiency in the preamble or objects section.[54] For example, the *Information Privacy Act 2000* (Vic) has an objects clause covering such matters as balancing the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector.[55] The Act then requires the Privacy Commissioner to have regard to the objects of the Act in the performance of his or her functions and the exercise of his or her powers under the Act.[56]

Submissions and consultations

46.40 In DP 72, the ALRC identified support in submissions and consultations for the requirement that the Privacy Commissioner have regard to the matters set out in s 29 of the *Privacy Act*. These include, most importantly, the balance between protecting individual privacy, the desirability of a free flow of information and minimising compliance costs for government and business.[57]

46.41 The ALRC supports the requirement that the Commissioner continue to have regard to such matters when exercising his or her functions. However, given the

---

50 Explanatory Memorandum, Privacy Bill 1988 (Cth), 37.

51 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 28.

52 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007.

53 *Privacy Act 1993* (NZ) s 14. See also *Information Privacy Act 2000* (Vic) s 60.

54 This is the approach taken in a number of jurisdictions, including: *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 3; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recitals 2, 3, art 1. See also the Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

55 *Information Privacy Act 2000* (Vic) s 5.

56 Ibid s 60.

57 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007.

ALRC's proposal to introduce an objects clause that draws on similar themes to those set out in s 29—particularly the requirement to balance the public interest in protecting the privacy of individuals with other public interests[58]—the ALRC proposed in DP 72 that, rather than a separate section, the Commissioner should have regard to the matters set out in the proposed objects clause.[59]

46.42 A number of stakeholders, including the OPC, supported this proposal.[60] PIAC suggested that the requirement for the Commissioner to have regard to the objects clause will 'lend weight to the objects clause and facilitate statutory interpretation'. Picking up on the Australian Privacy Foundation's submission to IP 31 that successive Privacy Commissioners appear to have interpreted s 29(a) as limiting their ability to perform the role of public advocate and champion of privacy, PIAC suggested that requiring the Commissioner to have regard to the objects of the Act, which includes promoting the protection of individual privacy, 'should lead to greater focus on these roles'.[61]

46.43 In contrast, the Australian Direct Marketing Association did not support the introduction of an objects clause, and thus submitted that this proposal was unnecessary.[62]

ALRC's view

46.44 The ALRC recommends in Chapter 5 that the *Privacy Act* should be amended to include an objects clause.[63] In that recommendation, the ALRC suggests objects that draw on similar themes to those in s 29, including to implement Australia's obligations at international law relating to privacy and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests. The objects clause also lists, as one of the purposes of the Act, to promote the protection of individual privacy.

46.45 Section 29 should be amended to require the Commissioner to have regard to the recommended objects of the Act in performing his or her functions and exercising his or her powers. This is consistent with a purposive approach to statutory interpretation,

---

58 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–4.

59 Ibid, Proposal 43–3.

60 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; 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; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

61 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

62 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

63 Rec 5–4.

which requires that, in interpreting a provision of an Act, a construction that promotes the purpose or object underlying the Act should be preferred to a construction that would not promote that purpose or object.[64]

46.46 Aligning the matters to which the Privacy Commissioner must have regard with the objects of the *Privacy Act* ensures that everyone interpreting, applying and attempting to understand the Act—whether they are agencies, organisations, consumers, lawyers, academics or the OPC itself—has regard to the same set of objects. By moving the factors set out in s 29 to the objects clause, the Act effectively indicates that, not only are the enumerated factors critical in influencing the Privacy Commissioner's administration of the Act, they are also critical in directing the general public's understanding and interpretation of the Act.

Recommendation 46–3 The *Privacy Act* should be amended to provide that the Privacy Commissioner must have regard to the objects of the Act, as set out in Recommendation 5–4, in the performance of his or her functions and the exercise of his or her powers.

Accountability mechanisms

46.47 The Privacy Commissioner and the OPC are subject to a number of accountability mechanisms to ensure that decisions made, and conduct engaged in, by the Commissioner and the OPC are legal and correct. These mechanisms include judicial review, merits review and review by the Commonwealth Ombudsman.

46.48 In addition to the review rights that, as discussed below, are primarily held by individuals (in the sense that an individual can initiate them through making a complaint or instituting proceedings), the Commissioner is also subject to another form of accountability—that is, the Commissioner is subject to parliamentary scrutiny with regard to the substance of legislative instruments issued by the Commissioner. Most of the binding instruments issued by the Commissioner—such the s 17 Tax File Number Guidelines and Public Interest Determinations[65]—are 'disallowable instruments', which means they are subject to parliamentary oversight and disallowance under the *Legislative Instruments Act 2003* (Cth). This provides further oversight and scrutiny of the substance of decisions made by the Commissioner.

---

64 *Acts Interpretation Act 1901* (Cth) s 15AA.

65 Other disallowable instruments issued by the OPC include the *Credit Reporting Code of Conduct*, and determinations made under Part IIIA. Note that privacy codes approved under Part IIIAA of the *Privacy Act* are legislative instruments but are not subject to disallowance by Parliament: see *Legislative Instruments Act 2003* (Cth) s 44(2), item 44; *Legislative Instruments Regulations 2004* (Cth) sch 2, item 8.

Judicial review

46.49 Complainants and respondents may apply under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (ADJR Act) to the Federal Court or Federal Magistrates Court for a review of 'administrative decisions', or 'conduct' preparatory to the making of a decision by the Privacy Commissioner under the *Privacy Act*.[66]

46.50 The ADJR Act provides an aggrieved person with broad grounds to apply for review. These grounds include a breach of natural justice; error of law; and an improper exercise of power, which includes having an improper purpose, taking an irrelevant consideration into account, failing to take a relevant consideration into account, an abuse of power and unreasonableness.[67]

46.51 Judicial review is to be distinguished from merits review. Under the ADJR Act, the court reviews the legality of the process followed to make the decision, not the substance of the decision (which is the subject of merits review). The court cannot hear the matter afresh or substitute the decision of the Commissioner with its own. If the court finds that the grounds for review are made out, it can make an order setting aside or quashing the decision and can remit the matter back to the Privacy Commissioner for further reconsideration according to law.[68]

46.52 Matters that could be the subject of an application for review under the ADJR Act include a decision not to investigate (or investigate further) a privacy complaint under s 41, a decision not to make a determination under s 52, and a failure to give reasons to a person adversely affected by a decision of the Commissioner.[69]

Merits review

46.53 As noted above, merits review is concerned with the substance of a decision and, in particular, whether the decision was the correct or preferable decision. There are very limited rights to merits review under the *Privacy Act*. There is a right to apply to the Administrative Appeals Tribunal for a review of the Commissioner's decision to refuse to approve the medical research and genetics guidelines under ss 95, 95A and 95AA of the *Privacy Act*.[70]

---

66 *Administrative Decisions (Judicial Review) Act 1977* (Cth) ss 3, 5, 6.

67 Ibid ss 5, 6.

68 Ibid s 16. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 129.

69 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 129; *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 16.

70 See *Privacy Act 1988* (Cth) ss 95(5), 95A(7), 95AA(3). Under s 95A(7), an application may also be made to the Administrative Appeals Tribunal for review of a decision of the Commissioner to revoke an approval of guidelines.

46.54 Secondly, merits review is available in respect of determinations against agencies, but only in relation to decisions made to include or not include a declaration for compensation or costs.[71] Merits review is not available for other decisions made by the Privacy Commissioner in the complaints process. For instance, there is no right to merits review of a decision by the Commissioner under s 41 of the Act not to investigate a complaint, or to cease investigations, on the basis that the Commissioner considers that the respondent has dealt adequately with the complaint—regardless of whether the complainant is satisfied with the respondent's response.[72]

Commonwealth Ombudsman

46.55 The Commissioner and the OPC are also subject to review by the Commonwealth Ombudsman with respect to 'a matter of administration'.[73] The Ombudsman is an independent statutory office holder who can investigate administrative actions of Australian Government officials and agencies, such as the OPC, either on receipt of a complaint or on the Ombudsman's own motion. The Ombudsman investigates and resolves disputes through consultation and negotiation, and, where necessary, by making formal, non-binding recommendations to senior levels of government. The type of actions the Ombudsman may report on include where the action: appears to have been contrary to law; was unreasonable, unjust, oppressive or improperly discriminatory; or was otherwise, in all the circumstances, wrong.[74]

46.56 The Ombudsman and the OPC entered into a memorandum of understanding (MOU) in November 2006. The MOU addresses a number of issues and is intended to ensure, among other things, that complaints made to one party about the other are handled efficiently and fairly.

ALRC's view

46.57 In DP 72, the ALRC identified stakeholder views on whether the accountability measures to which the OPC is subject under the *Privacy Act* are appropriate. While the issue of merits review was raised by several stakeholders (and is addressed in detail in Chapter 49), any significant concerns about the other accountability measures were not addressed in submissions.

46.58 The current accountability mechanisms of judicial review and review by the Commonwealth Ombudsman are appropriate. The fact that the Commissioner's decisions are subject to judicial review is an important oversight mechanism to ensure the legality of the exercise of the Commissioner's powers and that proper processes are

---

71 Ibid s 61. Merits review is discussed in detail in Ch 49.

72 See the concerns raised about this point in Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 138–139.

73 *Ombudsman Act 1976* (Cth) s 5; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 128.

74 *Ombudsman Act 1976* (Cth) s 15(1). There are a number of other circumstances set out in this section.

followed. The oversight by the Ombudsman is consistent with other federal regulators, and provides a necessary avenue for individuals who have a complaint against the administrative workings of the OPC.

46.59 The current rights to merits review, however, are not sufficient, particularly in relation to complaint determinations. The concerns raised by stakeholders about the inability to challenge the merits of the Commissioner's decisions are addressed in Chapter 49, with a recommendation made to provide merits review of determinations made by the Commissioner under s 52 of the *Privacy Act*.[75]

Criminal liability

Background

46.60 The Commissioner and his or her staff and delegates are subject to criminal liability in some circumstances. It is an offence for the Commissioner or a member of his or her staff (present and past) to disclose, use or make a record of information acquired about a person in the performance of that role, other than to do something permitted or required by the *Privacy Act*.[76] Such a person is not obliged to divulge or communicate that information except as required or permitted by the *Privacy Act*.[77] Similar secrecy provisions are found in other federal legislation and state privacy legislation.[78]

ALRC's view

46.61 In DP 72, the ALRC noted that the OPC supported the retention of the above provisions. The OPC submitted that these were consistent with secrecy and non-disclosure provisions in other Commonwealth legislation.[79] The ALRC has concluded that the current secrecy provisions are appropriate and has not made any recommendations on these matters.[80] The liability of the Commissioner to criminal sanctions for disclosure of certain information is appropriate and the provisions, as noted above, are consistent with other relevant legislation.

---

75 Rec 49–7.

76 *Privacy Act 1988* (Cth) s 96(1), (3). The offence is punishable by a penalty of $5,000 or imprisonment for one year, or both. Note that the OPC released its new layered privacy policy (which sets out its personal information-handling practices) in August 2006: Office of the Privacy Commissioner, *Privacy Policy* (2006).

77 *Privacy Act 1988* (Cth) s 96(2), (4).

78 See, eg, *Ombudsman Act 1976* (Cth) ss 35, 35A; *Migration Act 1958* (Cth) s 377; *Privacy and Personal Information Protection Act 1998* (NSW) s 67; *Information Privacy Act 2000* (Vic) s 67.

79 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

80 This issue was not raised in submissions other than by the OPC.

Immunity

Background

46.62 The Commissioner, and any person acting under his or her direction or authority, has immunity from civil action for acts done in good faith in the exercise of any power conferred by the *Privacy Act*.[81] This immunity also extends to an adjudicator under an approved privacy code and his or her delegate.[82] Privacy legislation in state, territory and overseas jurisdictions provides similar immunities to privacy commissioners,[83] and precedent for immunity can also be found in the *Ombudsman Act 1976* (Cth).[84]

46.63 The *Privacy Act* also provides that civil action will not lie against a person in respect of loss, damage or injury suffered by another person because of certain acts done in good faith. These acts are: the making of a complaint under the Act or under an approved code; the acceptance of a complaint under s 40(1B); or the making of a statement to, or giving information to, the Privacy Commissioner.[85] Similar immunity for complainants can be found in privacy legislation in Australian states and territories.[86]

46.64 In addition, persons who give information, produce a document or answer a question when directed to do so by the Commissioner are not liable to penalties under other Acts.[87]

Submissions and consultations

46.65 In DP 72, the ALRC identified support in submissions and consultations for the scope of immunities conferred on the Privacy Commissioner, adjudicators and other persons by the *Privacy Act*. The OPC supported the continuation of the immunity from civil actions provided to the Commissioner (or code adjudicator) and their delegates and also supported the protection from civil action provided to complainants. It explained that 'this is fundamental to providing individuals with an opportunity to freely raise a complaint without concern that they may be liable for defamation or other civil action'.[88]

---

81 *Privacy Act 1988* (Cth) s 64(1).

82 Ibid s 64.

83 For examples in other Australian privacy legislation, see *Privacy and Personal Information Protection Act 1998* (NSW) s 66; *Information Act 2002* (NT) s 151. For examples in overseas jurisdictions, see *Privacy Act* RS 1985, c P-21 (Canada) s 67; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 22; *Crown Entities Act 2004* (NZ) s 121.

84 *Ombudsman Act 1976* (Cth) s 33.

85 *Privacy Act 1988* (Cth) s 67.

86 *Privacy and Personal Information Protection Act 1998* (NSW) s 66A; *Information Privacy Act 2000* (Vic) s 66; *Information Act 2002* (NT) s 152.

87 *Privacy Act 1988* (Cth) s 44(5).

88 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

46.66 The Australian Privacy Foundation described these immunities as important and suggested that 'the law should confirm that the protection extends to bodies bringing representative complaints and otherwise drawing privacy compliance issues to the attention of the Commissioner and the public'.[89]

ALRC's view

46.67 The current immunity afforded to the Privacy Commissioner and code adjudicators, and their delegates, is appropriate and the ALRC does not make any recommendations for reform in this area.

46.68 The ALRC does not recommend any changes to the current formulation in s 67 of the *Privacy Act*, which provides protection from civil action to a person who, in good faith, makes a complaint under this Act. A complaint can only be made under s 36 of the Act, whether it is an IPP complaint, an NPP complaint, or a representative complaint.[90] A person or body who lodges a representative complaint under s 36 would enjoy protection from civil action where the act was done in good faith, because the protection in s 67 does not distinguish between the type of complaint made or the person who made the complaint; it applies to the act of making the complaint.

46.69 The ALRC notes, however, that there does not appear to be any guidance on the OPC website concerning the protection offered to complainants who make complaints in good faith. It would be useful for the OPC to make this protection clear in the document setting out its complaint-handling policies and procedures, which is the subject of Recommendation 49–8. This is particularly important given that, as recognised by the OPC, the protection is fundamental to ensuring that complainants feel safe in making complaints. It would be helpful to indicate clearly in the document setting out the OPC's complaint-handling policies and procedures that s 67 applies to individuals and bodies bringing representative complaints in the same way that it applies to individual complainants.

46.70 The *Privacy Act* does not need to be amended to confirm that the protection from civil action extends to bodies that otherwise draw privacy compliance issues to the attention of the Commissioner and the public.[91] In relation to issues brought to the attention of the Commissioner, s 67(b) already makes it clear that the protection from civil action extends to making a statement or giving a document or information to the Commissioner, whether or not required by s 44 of the *Privacy Act*.[92] This too, however,

---

89 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

90 See the respective definitions of each in *Privacy Act 1988* (Cth) s 6(1).

91 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

92 Note also that the Explanatory Memorandum to the Privacy Bill explained that s 67 'precludes a person from being sued for lodging a complaint with the Commissioner or providing him/her with information where those acts are done in good faith': Explanatory Memorandum, Privacy Bill 1988 (Cth), 59.

could be clarified further in the recommended complaint-handling policy and procedures document.

46.71 In relation to the suggestion that issues brought to the attention of the public also should attract immunity, it is the ALRC's view that such protection is not justified. The ALRC is not aware of examples of such protection being offered for disclosures to the public in any other privacy legislation. The OPC is the appropriate body with which to raise compliance issues. If a body wants to disclose issues to the public directly, then it should bear the risk.

Privacy Advisory Committee

Composition

46.72 The *Privacy Act* establishes a Privacy Advisory Committee (Advisory Committee) consisting of the Commissioner and not more than six other members, of which the Commissioner is convenor.[93] The Governor-General appoints members (other than Privacy Commissioner) as part-time members who hold office for up to five years. Members are not remunerated for their service, but enjoy similar protections as the Commissioner against removal,[94] and have an obligation to disclose any conflicts of interest.[95]

46.73 The *Privacy Act* provides membership criteria for the Advisory Committee in two ways. First, it specifies that officers, employees and staff of the Commonwealth must never be in the majority on the Advisory Committee.[96] Secondly, it provides a list of membership criteria.[97] The Advisory Committee is currently constituted by the Commissioner and six members.[98] Membership of the Committee was developed 'to represent a variety of community interest groups'[99] and must include representatives with experience in industry, commerce or government, trade unions, electronic data processing, social welfare and the promotion of civil liberties.[100]

46.74 No changes or additions were made to the membership criteria of the Advisory Committee following the introduction of the credit reporting provisions in 1990 or following the inclusion of the private sector provisions in 2000.

---

93 *Privacy Act 1988* (Cth) s 82(1)–(5). See also s 87 regarding meetings of the Advisory Committee.
94 Ibid s 85.
95 Ibid s 86.
96 Ibid s 82(6).
97 Ibid s 82(7).
98 See Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 14 May 2008.
99 Explanatory Memorandum, Privacy Bill 1988 (Cth), 4.
100 See Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 14 May 2008. Members of the Advisory Committee have been drawn from universities, PIAC, the Australian Consumers' Association, the Australian Chamber of Commerce and Industry, the Australian Information Industry Association and the HREOC.

Functions

46.75 The *Privacy Act* specifies that the Advisory Committee has functions to advise the Commissioner (whether or not requested) on matters relevant to the Commissioner's functions and recommend material for inclusion in guidelines to be issued by the Commissioner. It is also empowered to engage in and promote community education and consultation for the protection of individual privacy, subject to any directions given by the Commissioner.[101]

46.76 The OPC sets out on its website the terms of reference for the Advisory Committee, which are based on the functions set out in the *Privacy Act*. The OPC notes that the terms of reference 'assume a strategic advisory role' for the Advisory Committee and include:

- advising the Privacy Commissioner on privacy issues, and the protection of personal information;
- providing strategic input to key projects undertaken by the Privacy Commissioner;
- fostering collaborative partnerships between key stakeholders to promote further the protection of individual privacy;
- promoting the value of privacy to the Australian community, business and government; and
- supporting office accountability to external stakeholders.[102]

46.77 In its most recent annual report, the OPC described the Advisory Committee as acting 'as an external reference point that supports the Commissioner in gaining access to the broad views about privacy in the private sector, government and the community at large'.[103] In the past, the Advisory Committee has assisted the OPC by providing strategic advice about such matters as the review of the private sector provisions of the *Privacy Act* in 2004–05,[104] and the 25th International Conference of Data Protection and Privacy Commissioners in 2003–04.[105] The Advisory Committee has also provided

---

101 *Privacy Act 1988* (Cth) s 83.

102 Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 14 May 2008.

103 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 38–39.

104 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 29.

105 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 47.

input into guidelines developed by the OPC, as well as advice about the OPC's complaint processes and the publication of complaint case notes.[106]

46.78 The Privacy Commissioner can convene such meetings of the Advisory Committee as he or she considers necessary for the performance of the Committee's functions.[107]

Submissions and consultations

46.79 In DP 72, the ALRC noted that there was some dissatisfaction with the structure and functions of the Advisory Committee, however, stakeholders in general supported its continuation.

46.80 In relation to the general functions and powers of the Advisory Committee, the OPC submitted that it supported the continuation of the Advisory Committee in its current role as an independent advisory body. The OPC considered that the Committee's powers and functions are appropriate and found that the Committee provides valuable input into policy development and general strategic discussion.[108]

46.81 The Australian Privacy Foundation submitted that:

> The Privacy Advisory Committee may perform a useful function 'behind the scenes', but it is almost invisible to the public. Members do not seem to have seen themselves as accountable to the constituencies which might be inferred from the criteria for appointment and have rarely sought to consult with constituencies.
>
> The objectives of the Advisory Committee might be better performed by separate committees representing business, government and consumer interests respectively, with independent secretariats and public reporting requirements.[109]

46.82 In terms of additional functions, the National Association for Information Destruction submitted that the Advisory Committee could have a role in establishing a standard for secure document destruction.[110]

46.83 Stakeholders also commented on the membership criteria of the Advisory Committee. The OPC submitted that such criteria should be reviewed and updated to reflect current business, community and government environments. In particular, the OPC expressed strong support for the introduction of an explicit requirement that a health sector representative be included on the Advisory Committee given the

---

106 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 29; Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 47; Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 23.

107 *Privacy Act 1988* (Cth) s 87.

108 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

109 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

110 National Association for Information Destruction, *Submission PR 133*, 19 January 2007.

community concern regarding health privacy.[111] Another stakeholder went further and suggested there be two designated positions for the health sector: a consumer (from an advocacy organisation) and a practitioner.[112]

46.84 The OPC also suggested that the criteria be amended to require separately the inclusion of a member with high-level experience in industry or commerce *and* a member with experience in public administration or government, rather than combining these categories.[113]

Inclusion of a health representative

46.85 Following a number of suggestions that the categories of persons for appointment be expanded—and in particular, by the inclusion of a representative from the health sector—the ALRC proposed that the requirements for the composition of the Privacy Advisory Committee be amended to require the appointment of a person to represent the health sector and expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven.[114]

46.86 All stakeholders who commented on the addition of a health sector representative to the Committee supported the proposal.[115] For example, Avant Mutual Group Ltd submitted that 'given the very significant amount of health information generated by Australia's health sector and the important areas of scientific/medical research and genetics it is necessary to have a person represent the health sector'.[116]

---

111 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

112 Confidential, *Submission PR 134*, 19 January 2007. The Australian Privacy Foundation's submission to the Senate Legal and Constitutional Reference Committee inquiry into the *Privacy Act* also recommended that a separate position be 'reserved' for a representative of health issues, given the importance of the issue: Australian Privacy Foundation, *Supplementary Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988 concerning the Privacy Advisory Committee*, 1 March 2005, 3.

113 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

114 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 43–4.

115 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; Consumer Action Law Centre, *Submission PR 510*, 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; 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. The Australian Direct Marketing Association 'does not disagree' with this proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

116 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

46.87 While strongly supporting the appointment of a health representative to the Privacy Advisory Committee, one stakeholder suggested that the terminology of 'representative' in relation to members of the Committee should be reconsidered. Rather than appointing representatives, it was suggested that members with expertise relevant to a particular sector should be appointed to bring their particular knowledge and experience to the Committee. Importantly, such members should 'be required to exercise their functions so as to promote the achievement of the objects of the *Privacy Act* more broadly, rather than simply "representing" a sectoral view'.[117]

46.88 Stakeholders also suggested other members that should be included in the composition of the Committee, including a law enforcement representative[118] and a consumer sector representative.[119]

Updating language

46.89 In its submission to IP 31, the OPC suggested that the terminology used in the membership criteria—such as requiring a person with extensive experience in 'electronic data-processing'—should be updated to reflect better current data-handling practices.[120] Having regard to the fact that the term 'electronic data-processing' is not a term used throughout the *Privacy Act*,[121] the ALRC canvassed some alternative terminology, including 'information technology' or 'information and communication technologies'.

46.90 The term 'information technology' is generally understood to mean 'the use of computers to produce, store and retrieve information'[122] and encapsulates the notion of 'electronic data-processing'.[123] 'Information and communication technologies' is a modern development on 'information technology' and is intended to broaden the term explicitly to include all types of electronic communications. The term has been used to describe how information is 'produced, collected, sorted, filtered, transmitted, communicated, interpreted and stored'[124] and is used by a number of organisations throughout the world, including the European Commission, the World Bank, and the Organisation for Economic Co-operation and Development. The ALRC proposed that

---

117 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
118 Australian Federal Police, *Submission PR 545*, 24 December 2007.
119 Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.
120 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
121 'Electronic data-processing' is in fact only used in s 82(7)(c) of the *Privacy Act 1988* (Cth). 'Data processing' is used once in the *Privacy Act*, in s 27(1)(c). The use of 'processing' has its heritage in the Council of Europe Convention: see *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force generally on 1 October 1985).
122 *Macquarie Dictionary* (online ed, 2007).
123 The ALRC notes that the OPC website already refers to 'information technology' in describing the range of perspectives on the Advisory Committee: see Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 14 May 2008.
124 Commonwealth Scientific and Industrial Research Organisation, *Information and Communication Technology Overview* (2007) <www.csiro.au/org/ICTOverview.html> at 31 July 2007.

the term 'electronic data-processing' should be changed to 'information and communication technologies', to reflect more contemporary practices and parlance.[125]

46.91 Several stakeholders expressed support for the proposal to change the wording of 'electronic data-processing' to 'information and communication technologies'.[126]

ALRC's view

46.92 The Privacy Advisory Committee should continue in its current form, but with some amendments to the membership criteria. As statutory appointees, the members enjoy independence and protection from removal, allowing them to express views without fear or favour. Leaving the members as statutory appointments by the Governor-General insulates the Commissioner from allegations of bias in relation to a particular appointment. The Commissioner, however, may still make recommendations for appointments to the appropriate minister.

46.93 In order to give the Commissioner additional flexibility, however, the ALRC recommends that the Commissioner be given an express power to establish expert panels to assist with specific projects. This is discussed further below.

46.94 In terms of changes to the existing structure of the Privacy Advisory Committee, given the significance of privacy in the health sphere and the impact of health privacy on every member of the community, it is appropriate that a health perspective is represented on the Advisory Committee.[127]

46.95 It is not necessary that the membership criteria in s 82(7)(a) (industry or government representative) be separated. While the ALRC sees a benefit in having a government *and* industry representative on the Committee, representatives from both government and business can be appointed under the current membership structure. The Act only specifies five categories of members but allows the appointment of six members. Specifying six categories of membership (that is, including the new health category) and allowing for the appointment of seven members in addition to the Commissioner could be used to achieve the same result.

---

125 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 43–4.

126 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; 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.

127 The ALRC notes that under the current criteria, a health representative could be appointed within the ambit of the social welfare representative. However, it is the ALRC's view that it would be more beneficial to fill this criterion with a representative from the social and community welfare sector more generally, and to require, in addition to that member, a further member representing the health sector.

46.96 There are, however, two alternative approaches on this issue that could be adopted. The first is to separate the membership criteria and allow for one appointment per category (that is, specify seven categories and allow for seven members). The second is to separate the membership criteria, which would create seven categories of membership, and allow for the appointment of one member per category plus one member at large—equalling eight members together.

46.97 If the membership category in s 82(7)(a) was separated, the second option is preferable to the first, as it retains the flexibility to appoint persons beyond the confines of the membership criteria in the Act and allows for the appointment of more than one person to a membership category. The ALRC is concerned, however, that the second option increases the size of the Committee, which may affect the functioning and flexibility of the body itself, and may shift the preponderance of views on the Committee to the regulated entities—that is, to the government, business, health and data-processing sectors. While the Act specifies that a majority of appointed persons cannot be officers or employees of the Commonwealth, there is no such limitation against business or industry views.

46.98 Given the recommended objects of the Act, it is important that the Advisory Committee provide the Commissioner with a balanced range of views from both the regulated entities and from consumer and privacy advocates. The current compound category in s 82(7)(a), therefore, should be retained.

46.99 In relation to the other membership criteria put forward by stakeholders, those suggestions could be addressed under the existing membership criteria. It is important to keep the criteria at a high level. This enables representation from a variety of backgrounds and stakeholders discussed below. If specific expertise is required for a particular project, expert panels could be utilised.

46.100 With regard to terminology, the reference to 'electronic data-processing' in the membership criterion should be replaced with 'information and communication technologies', to reflect more contemporary practices and parlance. The ALRC prefers 'information and communication technologies' to 'information technology', as it is broader and encapsulates more clearly the notion of electronic communications.

Recommendation 46–4 The *Privacy Act* should be amended to make the following changes in relation to the Privacy Advisory Committee:

(a) expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven;

(b) require the appointment of a person who has extensive experience in health privacy; and

(c) replace 'electronic data-processing' in s 82(7)(c) with 'information and communication technologies'.

Expert panels

Background

46.101 In considering whether the current structure and role of the Privacy Advisory Committee is appropriate, the ALRC canvassed two main options for reform.

46.102 The first was to retain the current structure of the Committee, but make any necessary amendments to the membership requirements to reflect contemporary issues and community concerns. The second option was to change the Committee's legislative structure to make it a more flexible, informal body with a more projects or inquiry-oriented role. This could involve changing the appointment process, so that members are not statutory appointees for a set term, but are appointed by the Privacy Commissioner. Instead of mandating membership criteria, the Act could require that the Committee is broadly representative of the general community and set out a non-exhaustive list of criteria to achieve broad representation. This kind of membership structure would give the OPC flexibility to set up an Advisory Committee with specific expertise to assist with a particular project. An example of this model is found in the *Human Rights and Equal Opportunity Commission Act 1986* (Cth).[128]

46.103 Given the support for the continuation of the Privacy Advisory Committee in its current form, with some amendment to the membership criteria, the ALRC developed a compromise between these two options. While proposing the necessary changes to the Committee in order to make it a more relevant body, the ALRC also proposed that the Commissioner be empowered to establish expert panels at his or her discretion.[129] While recognising it was not necessary to include such a power in the Act, the ALRC's preliminary view was that an express power would be consistent with the legislative approach adopted with the Privacy Advisory Committee.

128 *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 17.

129 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 43–5.

Submissions and consultations

46.104 A number of stakeholders expressed support for this proposal.[130] PIAC noted other proposals made by the ALRC in DP 72 for the Commissioner to issue guidance in highly specialised and complex areas, and suggested that:

> Temporary or standing panels of persons with expertise in these areas would be of great assistance to the Privacy Commissioner in formulating this guidance, especially where the relevant expertise may not be located within OPC itself.[131]

46.105 In contrast, the OPC disagreed with the ALRC's proposal, submitting that 'as the Privacy Commissioner may already do so, it is unnecessary to amend the *Privacy Act* to empower the Privacy Commissioner to establish expert panels at his or her discretion to advise the Privacy Commissioner'. The OPC noted that it currently convenes expert panels as required, providing the example of the Health Privacy Forum, whose members provide a range of health expertise to the Commissioner.[132]

ALRC's view

46.106 Empowering the Privacy Commissioner to establish expert panels provides a valuable tool to deal with difficult and emerging areas of privacy regulation. While the ALRC recognises that the OPC already convenes expert panels without an express power, there is an advantage to setting out clearly that power in the *Privacy Act*. This is particularly the case as the Act already specifies the establishment and constitution of the Privacy Advisory Committee; it would be inconsistent to not also specify the Commissioner's power to establish expert panels.

46.107 The use of expert panels could address some of the concerns raised by stakeholders about a lack of more specific expertise on the Advisory Committee. For example, as noted above, the National Association for Information Destruction submitted that the Advisory Committee could have a role in establishing a standard for secure document destruction, in which case the Association suggested the Committee should include representatives from the secure information destruction industry.[133] In this instance, rather than mandating a permanent representative on the Advisory Committee, a better route would be to create an expert panel with representatives from the document destruction industry to provide expertise to the OPC in developing the standard.[134]

---

130 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; 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 Health and Medical Research Council, *Submission PR 397*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

131 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

133 National Association for Information Destruction, *Submission PR 133*, 19 January 2007.

134 See Ibid.

46.108 Expert panels could also be used to assist the OPC in the development of education and guidance materials relating to new and developing technologies. The work of such panels should be informed by the work of relevant government bodies in the area of information and communications technologies. This is discussed further in Part B of the Report.

Recommendation 46–5 The *Privacy Act* should be amended to empower the Privacy Commissioner to establish expert panels, at his or her discretion, to advise the Privacy Commissioner.

47. Powers of the Office of the Privacy Commissioner

Contents

Introduction

47.1 This chapter examines the functions vested in the Privacy Commissioner (Commissioner). These functions include powers to oversee the *Privacy Act 1988* (Cth) and to monitor compliance with the Act.[1] The chapter also discusses and makes recommendations aimed at clarifying the Commissioner's oversight powers and enhancing the use of privacy impact assessments (PIAs), audits and public interest determinations (PIDs) under the Act.

Oversight powers

47.2 The Commissioner's functions in overseeing the operation of the *Privacy Act* include: giving advice; providing research on, and monitoring of, technological developments; and conducting education. The Commissioner also has oversight functions in relation to tax file numbers and credit reporting.[2]

Advice functions

47.3 The Commissioner has several advisory functions under the *Privacy Act*. These are to:

- Provide advice to a minister, agency or organisation on any matter relevant to the operation of the *Privacy Act*.[3] A related function is to inform the Minister of action that needs to be taken by an agency to comply with the Information Privacy Principles (IPPs).[4]

1 The Commissioner's complaint-handling and enforcement powers are discussed in Chs 49 and 50.
2 The general approach of the *Privacy Act* is to state the Commissioner's 'functions' and give the Commissioner 'power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions': *Privacy Act 1988* (Cth) ss 27(2), 28(2), 28A(2).
3 Ibid s 27(1)(f). See also the equivalent function in credit reporting: s 28A(1)(f).
4 Ibid s 27(1)(j). Currently, the minister with responsibility for the *Privacy Act* is the Cabinet Secretary.

- Examine any proposal for data-matching or data linkage that may involve an interference with the privacy of individuals or may otherwise affect adversely the privacy of individuals, and to ensure that any adverse effects are minimised.[5]

- Examine any proposed enactment that would require or authorise acts or practices of an agency or organisation that might, in the absence of the enactment, be an interference with the privacy of individuals or which may otherwise affect adversely the privacy of individuals and to ensure that any adverse effects are minimised.[6]

- Make reports and recommendations to the Minister in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of individuals' privacy.[7]

- Provide advice to tax file number (TFN) recipients about their obligations under the *Taxation Administration Act 1953* (Cth) and on any matter relevant to the operation of the *Privacy Act*.[8]

- Provide advice to the adjudicator appointed under a privacy code on any matter relevant to the operation of the *Privacy Act* or the relevant privacy code.[9]

47.4 In 2006–07, the Commissioner used her advice functions to prepare 163 advices on significant policy issues, representing a 20% increase in the number of policy advices issued by the OPC in 2005–06. As described in the Annual Report of the Office of the Privacy Commissioner (OPC), the advices included: letters and emails to government departments, agencies and organisations on specific proposals; advice for guidance material published by the Commissioner; and advice for inclusion in other reports and published documents.[10] The OPC also provided 32 submissions to government departments and parliamentary inquiries on policy proposals or Bills before Parliament.[11]

Research and monitoring functions

47.5 Another aspect of the Commissioner's functions in overseeing the *Privacy Act* is undertaking research into, and monitoring developments in, data processing and computer technology (including data-matching and data linkage) to minimise their adverse effects on the privacy of individuals and to report to the Minister about the

---

5 Ibid s 27(1)(k).
6 Ibid s 27(1)(b). This power, and the related concept of privacy impact assessments, is discussed separately below.
7 Ibid s 27(1)(r). Currently, the minister with responsibility for the *Privacy Act* is the Cabinet Secretary.
8 Ibid s 28(1)(g).
9 Ibid s 27(1)(fa).
10 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 5.
11 Ibid, 6.

results of such research and monitoring.[12] The Commissioner also has the function of monitoring and reporting on the adequacy of equipment and user safeguards.[13]

Education functions

47.6 The Commissioner's oversight functions in relation to education include:

- promoting an understanding and acceptance of the IPPs and National Privacy Principles (NPPs) and of the objects of those principles;[14] and

- undertaking educational programs on the Commissioner's own behalf or in cooperation with other persons or authorities acting on behalf of the Commissioner, for the purpose of promoting the protection of individual privacy.[15]

47.7 The OPC has said that a factor likely to increase community confidence that individuals' rights are protected is 'raising awareness about individuals' privacy rights'.[16] To this end, the OPC provides information through its information hotline and its website (which contains various OPC publications). Visits to the OPC's website have increased each year.[17]

47.8 Considerable attention was given to the Commissioner's education power in the OPC review of the private sector provisions of the *Privacy Act* (OPC Review) and the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Senate Committee privacy inquiry). Overall, the submissions acknowledged that education by the OPC plays a vital part in promoting community awareness of privacy laws. It was suggested in several submissions that public awareness be raised, using either one-off or regular campaigns. It was also suggested that sectors of the community with low awareness of privacy rights be targeted, and that campaigns address not only individuals' rights, but also the rights and obligations of organisations.[18]

---

12 *Privacy Act 1988* (Cth) s 27(1)(c). Currently, the minister with responsibility for the *Privacy Act* is the Cabinet Secretary.

13 Ibid s 27(1)(q). The use of these powers in relation to new and developing technologies is discussed further in Part B.

14 Ibid s 27(1)(d).

15 Ibid s 27(1)(m).

16 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 105.

17 See Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 32–33.

18 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 107–111. See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 145.

47.9 Both reviews called for the OPC to be funded adequately. It was said that this would facilitate a shift in focus from complaint handling to education. In the OPC Review, the OPC noted that 'since the implementation of the private sector provisions, the Office has shifted resources from its guidance and advice role to its compliance role to try to better manage and resolve the complaints received'.[19] It recognised, however, that 'organisations need more guidance'[20] and recommended that the Government consider specifically funding the OPC to undertake a systematic and comprehensive education program to raise community awareness of privacy rights and obligations.[21]

47.10 Following the OPC Review, the then Coalition Government made a commitment in 2006 to provide additional funding to the OPC over the next four years. In response, the OPC has stated that this could

> allow us to respond to calls from business and industry for greater assistance in meeting their obligations under the *Privacy Act*. Following on from recommendations made in my 2005 review of the private sector provisions of the *Privacy Act*, my Office will work closely with business and consumer representatives to develop guidance and educational material to assist organisations and individuals to better understand their rights and responsibilities under the *Privacy Act*.[22]

Submissions and consultations

47.11 In DP 72, the ALRC identified support in submissions and consultations for the OPC's oversight, advice and education roles. Concern was expressed by the OPC, however, that the current research and monitoring power is limited to researching computer technology. The OPC submitted that the reference in s 27(1)(c) to 'computer technology' is outdated and 'may inadvertently restrict the operation of this clause which the Office believes is intended to provide for research into technologies with a possible privacy impact, whether or not they are computer-based'.[23] Accordingly, the ALRC proposed that the power be broadened to include research more generally, by removing the word 'computer' in the function.[24]

---

19 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 5.

20 Ibid, 7.

21 Ibid, recs 26, 48. The Senate Committee privacy inquiry made a similar recommendation: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 19.

22 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 2–3.

23 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

24 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–1.

47.12 The ALRC received a number of submissions in support of the proposal to widen the Commissioner's research function to cover all technologies.[25] For example, the Department of Human Services submitted that the proposal 'will help encompass all present technologies that could possibly impact on an individual's privacy, thus making the *Privacy Act* more technology neutral'.[26]

47.13 DP 72 also identified concerns about the public nature of advice issued by the OPC and the exercise of the education function. In relation to the issuing of advice, the Consumer Credit Legal Centre (NSW) (CCLC) submitted that, while the Commissioner's legislative power to provide advice is appropriate, 'its exercise is not always effective nor does it always produce fair outcomes for consumers'.[27] In particular, the CCLC submitted that any advice given by the Commissioner in relation to any matter relevant to the operation of the Act should be made public, 'in order to ensure the transparency and fairness of OPC's operations'.

47.14 The exercise of the education function also drew comment from stakeholders. Several stakeholders commented on the apparent lack of priority given by the OPC to the education function and the need for more guidance from the OPC to encourage an understanding of, and compliance with, the privacy principles.[28] Stakeholders noted the preventative aspects of education—to reduce the potential for breaches of privacy and 'ill-informed reliance on privacy as a reason for refusing to take particular action'.[29]

47.15 In relation to public education, stakeholders commented on the 'utility of education materials in uplifting public confidence in, and awareness of, the OPC's ability to enforce privacy rights'.[30] Another stakeholder observed that lack of understanding of privacy regulation is often the source of complaints, with more education identified as a way to address this problem.[31] The public forums and consultations conducted, and submissions received by the ALRC in this Inquiry,

---

25 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; Australian Government Department of Human Services, *Submission PR 541,* 21 December 2007; GE Money Australia, *Submission PR 537,* 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007.

26 Australian Government Department of Human Services, *Submission PR 541,* 21 December 2007.

27 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. Similar comments were made in Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

28 Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

29 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. The NHMRC suggested that there is 'considerable anecdotal evidence that the appropriate handling of health information for important health care and health and medical research purposes is jeopardised by a generally inadequate understanding of the law': National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

30 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. See also Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

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

suggested low levels of awareness and understanding of privacy laws in the community. The ALRC received many stories of 'BOTPA' ('because of the *Privacy Act*') explanations being given as a reason for refusing a request for information or assistance from an agency or organisation.[32] While the extent to which such explanations are based on a proper understanding and application of the Act, rather than a deliberate excuse to avoid giving information, is not clear, education may help to increase understanding and lessen the reliance on BOTPA explanations.[33]

47.16 Some stakeholders suggested that industry bodies, schools and other institutions also should bear some responsibility to educate their members, students or constituencies about privacy obligations.[34] It was suggested, for example, that privacy should be taught in medical schools and in intern programs to ensure that medical students are aware of their obligations before they handle personal information about their patients.

47.17 The Cyberspace Law and Policy Centre submitted that the Privacy Commissioner's power under s 27 to report to the Minister on the exercise of his or her functions also should be broadened to allow reports to the public or to Parliament on all of the matters listed in the section (except those dealing with national security or similar considerations of confidentiality).[35]

47.18 Stakeholders supported the role of the Commissioner in providing education and guidance. The Australasian Compliance Institute suggested that the OPC should continue to take 'a leadership role' in relation to guidance and education at an agency, industry, and consumer level and it should maintain a consultative approach.[36] Similarly, the Federation of Community Legal Centres (Victoria) emphasised that this power needs to be exercised more extensively and in a targeted fashion in consultation with disadvantaged individuals, communities and their advocates, so that those who are most vulnerable to privacy breaches gain a better understanding of their rights and how they may be exercised effectively.[37]

---

32 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; H Ruglen, *Submission PR 39*, 27 June 2006; K Bottomley, *Submission PR 10*, 1 May 2006; T de Koke, *Submission PR 8*, 5 April 2006. See also Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006.

33 See Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

34 See Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

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

36 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

37 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007.

ALRC's view

47.19 The Commissioner's oversight functions provide important tools to: increase understanding of federal privacy law; contribute a privacy perspective to public debates; and establish dialogue on privacy issues between the OPC and agencies and organisations. These functions enable the Commissioner to be proactive in increasing awareness and understanding of privacy to prevent non-compliance. As discussed in Chapters 4 and 45, these functions enable the Commissioner to play a critical role in the ALRC's recommended regulatory model for privacy. These functions should be interpreted broadly, and resourced effectively.

47.20 The ALRC recommends one amendment to the Commissioner's oversight functions. The ALRC's view is that, given the serious impact technology can have on invading privacy or enhancing privacy protection, the Commissioner's research and monitoring function should be broad enough to enable the OPC to research and monitor all relevant technologies.[38] Some technologies may not come within an ordinary understanding of 'computer technology', yet still raise privacy issues. Biometrics is one example. The wording of s 27(1)(c) should be broadened to allow for research and monitoring of any pertinent technologies. This can be achieved most easily by removing the reference to 'computer'. Such an amendment is also consistent with the ALRC's recommendation that the privacy principles be technology neutral.[39]

47.21 As amended, this function provides the OPC with the specific power to call on its knowledge and expertise on privacy issues and conduct research into, for example, new and developing areas of technology. Research and reports to the Minister can provide an excellent medium to guide policy in these areas and to increase awareness of the issues raised by particular technologies. For these reasons, the ALRC recommends that the research power be broadened to explicitly empower the Privacy Commissioner to undertake research, and monitor developments in technology generally (as well as data-matching).

47.22 While the ALRC is not recommending reform of the OPC's advice function, the ALRC notes the concerns of stakeholders that advice should be timely and public. It is preferable, therefore, that advice (or a generic form of it) is made public if it is relevant to a broader audience and would increase understanding of the *Privacy Act*. It would not be reasonable, however, to require that all advice given by the Commissioner in relation to any matter relevant to the operation of the Act be made public. A minister or an agency may approach the Commissioner for advice on a confidential basis about Cabinet proposals, or an organisation may seek advice on proposals that are commercial-in-confidence or disclose an innovation or new project. Requiring such advice to be made public may discourage agencies and organisations from approaching

---

38 The ALRC recommends that the Commissioner use this research and monitoring function to consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations: Rec 10–1.

39 Rec 18–1.

the OPC, which would undermine the Commissioner's oversight and advisory functions.

47.23 The ALRC recognises the pivotal role education plays in a principles-based regime such as the *Privacy Act*. Compliance with such a regime is dependent on a shared understanding of what the principles mean and how they are to be applied. Education is also critical to raise awareness of privacy rights in the community; indeed, one of the recommended objects of the *Privacy Act* is to promote the protection of individual privacy.[40]

47.24 As compliance is ultimately the responsibility of the agency or organisation, it is important that industry groups and peak bodies perform a role in increasing awareness of privacy obligations and fostering compliance in their industries. The ALRC supports the involvement of industry bodies and authorities in undertaking education programs on the requirements of the *Privacy Act*, either in conjunction with, or in addition to, education programs undertaken by the OPC. Information sheets, fact sheets, and 'frequently asked questions' on industry websites can play an important role in assisting organisations understand their privacy obligations in an industry-specific manner.[41]

Recommendation 47–1 The *Privacy Act* should be amended to delete the word 'computer' from s 27(1)(c).

Guidelines

47.25 As discussed in Chapter 4, in a principles-based regime, guidance is often necessary to make the rights and obligations in the Act sufficiently certain and clear.[42] Guidance can be provided in a number of forms, including website information, 'frequently asked questions', education programs, and the Commissioner's oversight functions, discussed above. It also can be provided through the Commissioner's power to issue non-binding and binding guidelines under the *Privacy Act* and other legislation.

40 Rec 5–4.

41 An example of industry advice is a summary information sheet issued by the Real Estate Institute of Australia on Residential Tenancy Database Operators Regulations: see Real Estate Institute of Australia, *Residential Tenancy Databases and the Privacy Act 1988* (2007) <www.reia.com.au/documents/REIA_Summary_on_Amendments_Privacy_and_RTDs-August2007.doc> at 15 May 2008. The OPC has helped spread awareness of this information sheet by including a reference and a link to it on one of its Privacy Connections alerts.

42 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 14.

Power to issue non-binding guidelines

Section 27(1)(e) guidelines

47.26 The Commissioner has the power to prepare and publish guidelines to assist agencies and organisations to avoid acts or practices that may be interferences with, or affect adversely, the privacy of individuals.[43] The s 27(1)(e) guidelines are advisory only and are not legally binding. The guidelines are based on the OPC's understanding of how the *Privacy Act* works and indicate some factors the Commissioner may take into account when handling a complaint. Nothing in the guidelines limits how the OPC can handle complaints.[44]

47.27 The Audit Manual for the IPPs, published by the OPC, also addresses the status of guidelines and provides that 'in any privacy audit, the auditors may, at the discretion of the Privacy Commissioner, examine and report on the level of adherence to any such additional guidelines'.[45] Therefore, while guidelines issued under s 27(1)(e) are not determinative, they are often highly persuasive.

Privacy code guidelines

47.28 Specific provision is made for the Commissioner to prepare and publish guidelines regarding privacy codes. These may assist organisations to develop or apply approved privacy codes; relate to the making of, and dealing with, complaints under approved privacy codes; or discuss matters the Commissioner may consider in deciding whether to approve a code or a variation of an approved code.[46] The OPC published *Guidelines on Privacy Code Development* in September 2001.[47] These guidelines are binding in relation to complaint handling under a code but otherwise are advisory only.[48]

---

43 *Privacy Act 1988* (Cth) s 27(1)(e). There is an analogous power to prepare guidelines for the avoidance of acts or practices of a credit reporting agency or credit provider that may or might be interferences with the privacy of individuals: see *Privacy Act 1988* (Cth) s 28A(1)(e).

44 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 26. A similar approach is taken in the Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to Communicate or Transact with Individuals* (2001), 25; Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), i; Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), 3.

45 Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 5.

46 *Privacy Act 1988* (Cth) s 27(1)(ea).

47 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001). The OPC has undertaken to review the Code Development Guidelines: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 47.

48 *Privacy Act 1988* (Cth) s 18BB(3)(A)(ii).

Power to issue binding guidelines

Tax file numbers

47.29 In addition to the Commissioner's powers to issue non-binding guidelines, the Commissioner can issue 'binding' statutory guidelines under the *Privacy Act* and other Acts. For example, under s 17 of the *Privacy Act*, the Commissioner must issue guidelines concerning the collection, storage, use and security of TFN information.[49] These guidelines are made binding by virtue of s 18, which prohibits a file number recipient from doing an act or engaging in a practice that breaches the guidelines.[50]

47.30 The OPC issued Tax File Number Guidelines in 1992 and it has published an annotated version of the guidelines (including all amendments as at March 2004) on its website.[51] The Commissioner has a general power to evaluate compliance with TFN guidelines and may investigate an act or practice of file number recipients that may breach the guidelines.[52] File number recipients also can be audited to ascertain whether records of TFN information maintained by the recipient are in accordance with the s 17 guidelines,[53] which are discussed below.

Medical research guidelines

47.31 The *Privacy Act* also invests the Commissioner with the power to approve guidelines issued by the NHMRC in relation to medical research and genetic information under ss 95, 95A and 95AA.[54] Once approved, these guidelines are binding.

Other Acts

47.32 The Commissioner is specifically given the power to formulate and issue binding guidelines under s 12 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and s 135AA of the *National Health Act 1953* (Cth).[55]

Submissions and consultations

47.33 In DP 72, the ALRC proposed that the *Privacy Act* be amended so that binding guidelines issued by the Privacy Commissioner are renamed 'rules', to reflect that a breach of the rules is an interference with privacy under s 13 of the *Privacy Act*.[56] This would ensure that the difference between non-binding guidelines and binding guidelines was appropriately reflected in the language of the Act.

---

49 See also Ibid s 28(1)(a).
50 A breach of these guidelines constitutes an interference with the privacy of the individual: Ibid s 13(b).
51 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
52 *Privacy Act 1988* (Cth) ss 28(1)(f), s 28(1)(b).
53 Ibid s 28(1)(e).
54 These guidelines are discussed further in Chs 64, 65.
55 *Privacy Act 1988* (Cth) s 27(1)(p)–(pa).
56 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–2.

47.34 Stakeholders were unanimous in their support for this proposal.[57] The OPC, for example, submitted that the proposal had 'the potential to improve clarity regarding the binding nature of a document produced or recognised under the *Privacy Act*'.[58]

ALRC's view

47.35 The power to issue guidance is a critical part of regulating a principles-based regime such as the *Privacy Act*.[59] The Commissioner's function in s 27(1)(e), as currently drafted, is broad enough to enable the Commissioner to issue guidance on a range of matters, particularly when read in conjunction with the Commissioner's powers to provide advice, promote an understanding of the NPPs and IPPs, and undertake education programs. For these reasons, the ALRC is not recommending any reform to the guideline function.

47.36 Consistently, however, with the recommendation that the *Privacy Act* be redrafted to achieve greater clarity,[60] the ALRC recommends that the language used in the Act should be changed to reflect more accurately the binding or non-binding nature of the guidelines issued. Non-binding guidelines should continue to be called 'guidelines', as they provide a voluntary guide on ways to achieve the outcome set by the relevant privacy principle, without compelling directly a particular course of action. In contrast, where the guidelines provide rules for compliance, a breach of which constitutes an interference with privacy, then they should be called 'rules'. This recommendation will assist agencies and organisations to distinguish between guidelines that are merely advisory and those that operate as rules.

Recommendation 47–2 *The Privacy Act* should be amended to reflect that, where guidelines issued or approved by the Privacy Commissioner are binding, they should be renamed 'rules'. For example, the following should be renamed to reflect that a breach of the rules is an interference with privacy under s 13 of the *Privacy Act*:

---

57 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 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; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

59 See also Ch 4.

60 Rec 5–2. Note that, as the ALRC recommends that the existing ss 95 and 95A guidelines be abolished (see Ch 65), the ALRC has not included these guidelines in Rec 47–2 (although if they remain, they should be renamed 'rules' consistent with Rec 47–2). This language is also consistent with the approach taken in *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 229.

(a) Tax File Number Guidelines issued under s 17 of the *Privacy Act* should be renamed the *Tax File Number Rules*;

(b) Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs (issued under s 135AA of the *National Health Act 1953* (Cth)) should be renamed the *Privacy Rules for the Medicare Benefits and Pharmaceutical Benefits Programs*;

(c) Data-Matching Program (Assistance and Tax) Guidelines (issued under s 12 of the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth)) should be renamed the *Data-Matching Program (Assistance and Tax) Rules*; and

(d) Guidelines on the Disclosure of Genetic Information to a Patient's Genetic Relative should be renamed the *Rules for the Disclosure of Genetic Information to a Patient's Genetic Relative*.

Personal Information Digest

Background

47.37 The Commissioner has the function under s 27(1)(g) of maintaining and publishing annually a record of 'the matters set out in records maintained by record keepers in accordance with clause 3 of IPP 5'. Record keepers, in this context, are agencies; and the record is known as the Personal Information Digest (Digest). The matters that must be included in the Digest are:

- the nature of the records of personal information kept by or on behalf of the record keeper;
- the purpose for which each type of record is kept;
- the classes of individuals about whom records are kept;
- the period for which each type of record is kept;
- the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
- the steps that should be taken by persons wishing to obtain access to that information.

47.38 Currently, agencies provide their Digest entries to the OPC, which then makes them available on the OPC website.

Submissions and consultations

47.39 In DP 72, the ALRC identified support in submissions and consultations for changing the Digest requirements. A number of agencies submitted that the Digest entries were repetitive to prepare annually and not useful for the public, particularly given the increasing tendency of agencies to publish a privacy policy on their websites.

47.40 In DP 72, the ALRC proposed that the general notification principles currently located in the IPPs and NPPs should be consolidated and simplified into an 'Openness' principle.[61] The proposed principle would require an agency to produce a 'Privacy Policy' setting out the type of information currently required in the Digest entry, with some additions. The agency or organisation would be required to take reasonable steps to make its Privacy Policy available to an individual electronically, such as on its website, or in hard copy.[62]

47.41 The Cyberspace Law and Policy Centre did not disagree with the proposal to abolish the Personal Information Digest, which it acknowledged has rarely been used. It argued, however, that the OPC should prepare and publish a consolidated index of all Privacy Policies, which would allow public interest groups and the media to compare the policies.[63]

ALRC's view

47.42 The implementation of the recommendations in Chapter 24, dealing with the 'Openness' principle in the model UPPs, would obviate any need for the current requirement to prepare a Digest entry. It would also mean that the corresponding obligation on the Commissioner to prepare the consolidated Digest could be removed.

47.43 It is not necessary for the OPC to undertake a corresponding obligation in relation to Privacy Policies—that is, to prepare and publish on its website a consolidated index of all Privacy Policies. Such a process would be resource intensive and is unlikely to increase awareness of privacy policies more generally. In the current electronic environment, individuals seeking an agency's Privacy Policy are more likely to go to the agency's website than look on the OPC website. The key concern is that Privacy Policies should be readily available to members of the public, which would be achieved by the requirement to make them available without charge electronically; and, on request, in hard copy or in an alternative form accessible to individuals with special needs.[64]

---

61 See Ch 24.
62 Rec 24–2.
63 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
64 Rec 24–2.

Recommendation 47–3 Subject to the implementation of Recommendation 24–1, requiring agencies to develop and publish Privacy Policies, the *Privacy Act* should be amended to remove the requirement in s 27(1)(g) to maintain and publish the Personal Information Digest.

Privacy impact assessments

Background

47.44 PIAs have been the topic of much discussion in recent reviews of the *Privacy Act* and in privacy commentary more generally. The term 'privacy impact assessment' is not defined in the *Privacy Act*, nor is there a requirement for the Commissioner, or for an agency or organisation, to undertake a PIA. There is, however, a related function vested in the Commissioner, which is to examine and advise on a proposed enactment.[65] While the Commissioner may produce a PIA as a result of such an examination, the term 'privacy impact assessment' has come to refer to a more formalised assessment conducted by the relevant agency or privacy consultant, rather than by the Commissioner.[66]

Definition

47.45 The OPC suggests that a PIA is an assessment tool that 'tells the story' of the project from a privacy perspective. It describes the personal information flows in a project and analyses the possible impact on privacy of those flows.[67] Others have suggested a PIA is 'an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated'.[68]

47.46 It is suggested that PIAs are a form of proactive regulation that can help prevent privacy-intrusive legislation or projects from being implemented. In a principles-based regulatory regime, PIAs also can help 'marry the discretion allowed under the Act with a degree of accountability to the public where a significant privacy erosion will be caused'.[69] In addition, PIAs also may help 'tackle wider privacy issues such as

---

65 *Privacy Act 1988* (Cth) s 27(1)(b). Privacy Commissioners in other Australian jurisdictions have similar powers to examine and advise on the privacy impacts of proposed legislation. See, eg, the *Information Privacy Act 2000* (Vic) s 58(1); *Information Act 2002* (NT) s 86(1)(f); *Information Act 2002* (NT) s 86(1)(f). See also *Human Rights and Equal Opportunity Act 1986* (Cth) ss 11(1)(e), 46C(1)(d); *Disability Discrimination Act 1992* (Cth) s 67(1)(i); *Sex Discrimination Act 1984* (Cth) s 48(1)(f).

66 See, eg, the Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006); New Zealand Government Privacy Commissioner, *Privacy Impact Assessment Handbook* (2007); Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments—A Guide* (2004).

67 Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 4.

68 B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61, 62. See also the definitions of PIAs in Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.1].

69 B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61, 61.

intrusion'[70] and are seen by many as one of the key ways to address the possible privacy impact (whether negative or positive) of new or developing uses of technology.[71]

47.47 The most significant benefits of a PIA are achieved when it is integrated into the decision-making process for the project.[72] It has been suggested that the PIA must take place 'during the development of proposals when there is still an opportunity to influence the proposal'.[73] In this way, a PIA is to be distinguished from a privacy compliance audit. While both are proactive compliance measures, the latter examines the information-handling practices of an auditee 'that are in place at the time, as opposed to future proposals that the auditee might be contemplating'.[74] A PIA, in contrast, focuses on future projects.

Status in Australia

47.48 As noted above, the Commissioner can prepare a PIA when exercising the function of examining and advising on proposed enactments. While the Commissioner can report to the Minister about a proposed enactment and *must* report if directed to do so by the Minister,[75] the Minister is not required to obtain the OPC's advice in relation to proposed legislation or to act on any recommendations made by the OPC in a report to the Minister.[76] Similarly, there are no requirements in the *Privacy Act* for an agency to undertake a PIA. In the absence of a legislative directive, the OPC has said the incentive for conducting a PIA comes from the fact that 'the success of an agency's project will depend in part on it complying with legislative privacy requirements and how well it meets broader community expectations about privacy'.[77]

---

70 Ibid, 61.

71 See, eg, the Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005). See also B Stewart, 'Privacy Impact Assessment: Towards a Better Informed Process for Evaluating Privacy Issues Arising from New Technologies' (1999) 5 *Privacy Law and Policy Reporter* 147.

72 B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61. See also Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.3].

73 United Kingdom Government Information Commissioner's Office, *Evidence Submitted to the Home Affairs Committee Inquiry into 'The Surveillance Society?'* 23 April 2007, 6.

74 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 64. See also Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.7]; B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61.

75 *Privacy Act 1988* (Cth) s 31. Currently, the minister with responsibility for the *Privacy Act* is the Cabinet Secretary.

76 The Australian Government Department of the Prime Minister and Cabinet, *Legislation Handbook* (1999), [4.7(h)(vi)] provides that, in relation to legislative matters going before Cabinet, it is expected that the relevant department undertake other consultations in preparing the submission, including 'with the Privacy Commission [sic] if the legislation has implications for the privacy of individuals'.

77 Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 4.

47.49 To encourage agencies to undertake PIAs, the OPC produced a *Privacy Impact Assessment Guide* (PIA Guide), which provides detail on the nature, purpose and effect of a PIA. The PIA Guide contains modules for undertaking the PIA process. The PIA Guide notes that, while there is no formal role for the OPC in the development, endorsement or approval of PIAs, the OPC may be able to advise agencies on privacy issues arising throughout the assessment process.[78] The OPC often recommends that a department undertake a PIA as part of its advice on proposed enactments and policy submissions.[79]

47.50 The OPC has not prepared a similar guide for organisations, although the use of PIAs in the private sector was discussed in the OPC Review. It was suggested that organisations should use the PIA process 'to assess and avoid privacy risks inherent in many large scale projects using new technologies'.[80] Ultimately, the OPC did not recommend that organisations should be *required* to prepare, or obtain, a PIA. The OPC has subsequently noted that:

> it considers that the best way for organisations and government agencies to avoid interferences with privacy is for them to use a [PIA] to analyse the risks to privacy posed by new projects, technologies or rules and to address those risks before problems occur.[81]

47.51 The Senate Committee privacy inquiry went further and recommended that the *Privacy Act* 'be amended to include a statutory [PIA] process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information'.[82] The Australian Government did not agree with the Senate Committee's recommendation, noting that 'the Privacy Commissioner is developing a [PIA] process for use by agencies and considers that at this time a statutory process is not appropriate'.[83]

---

78 Ibid, 17.

79 See, eg, Australian Government Office of the Privacy Commissioner, *Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006*, 2; Office of the Privacy Commissioner, *Comments to the Attorney-General's Department on the Review of the Law on Personal Property Securities: Discussion Paper 1 Registration and Search Issues*, 1 February 2007, 3.

80 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 255–256.

81 S Jenner, 'The Impact of Computers on Privacy: A Virtual Story' (Paper presented at Striking A Balance: Computer Audit, Control and Security 2005 Conference, Perth, 23–26 October 2005).

82 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 5. This recommendation was not limited to agencies.

83 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), 2–3.

PIAs in other jurisdictions

Requirements imposed on agencies

47.52 A number of jurisdictions require agencies to prepare a PIA in certain circumstances. The Canadian government was the first federal government to make PIAs mandatory.[84]

47.53 Under the Canadian Government's Privacy Impact Assessment Policy, all federal departments and agencies must conduct a PIA 'for proposals for all new programs and services that raise privacy issues'.[85] Representatives of the Office of the Privacy Commissioner of Canada (Canadian Privacy Commissioner) must be involved at the earliest possible stage of the development of the PIA, and a copy of the PIA must be provided to the Canadian Privacy Commissioner and published on the internet.[86] The Canadian Privacy Commissioner's role is not to accept or reject projects, but 'to assess whether or not departments have done a good job of evaluating the privacy impacts of a project and to provide advice, where appropriate, for further improvement'.[87]

47.54 The Canadian Privacy Commissioner has explained that PIAs are important in the public sector because of the lack of control that individuals exercise over their own personal information. Whereas, in a commercial context, parties are free to enter transactions and define the terms of their exchange according to their respective interests, individuals are rarely in a strong bargaining position when it comes to the collection and use of their personal information by government. Because of this situation,

> government has a special trust relationship with citizens—a fiduciary duty to protect personal information under its charge. Performing PIAs constitutes one way that government institutions can honor that public trust, and in so doing earn the confidence of their clients and the public at large.[88]

47.55 Some Canadian provinces also encourage or require PIAs.[89] In addition, the *E-Government Act* in the United States requires that a PIA be undertaken, reviewed by the Chief Information Officer of the agency and, if practicable, published, before an

---

84 G Greenleaf, 'Canada Makes Privacy Impact Assessments Compulsory' (2002) 8 *Privacy Law and Policy Reporter* 190. This policy took effect on 2 May 2002.

85 Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy* (2002).

86 Ibid.

87 S Bloomfield, 'The Role of the Privacy Impact Assessment' (Paper presented at Managing Government Information: 2nd Annual Forum, Ottawa, 10 March 2004), 3–4.

88 Ibid, 2. The PIA Policy also came out of the Canadian Government's e-government initiatives, with the Policy identified as one of several tools designed to meet the challenge of assisting Canadians in understanding how the government handles their personal information and building trust in the government to handle such information responsibly, regardless of the service-delivery channel they choose to use—see Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy* (2002).

89 See, eg, the *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia) s 69(5); *Health Information Act 2000* RSA c H–5 (Alberta) ss 46, 64, 70, 71.

agency develops or procures a new information system or initiates a new collection of personally identifiable information.[90]

47.56 The Office of the Information Commissioner (UK) (UK Information Commissioner) has recently developed and released a PIA handbook, setting out a framework for conducting PIAs. The PIA process in the United Kingdom is not a legislative requirement, rather the Information Commissioner has noted that taking a 'proactive approach in the UK offers significant benefits by addressing privacy concerns and inspiring the public's trust and confidence in what happens to their personal information'.[91] The handbook, which is aimed at corporations and government agencies, states that a PIA should be considered when a proposal may give rise to public concerns about privacy (and those concerns would represent a significant risk for the project). It sets out a plan for conducting a PIA, including when stakeholders should be involved.[92] The handbook also stresses that reports of the PIA process should be open and transparent.

> A PIA Report should be written with the expectation that it will be published, or at least be widely distributed. If so, the report can fulfill [its] functions: accountability, post-implementation review, audit, input into future iterations of the PIA, and background information for people conducting PIAs in the future. [93]

Requirements imposed on organisations

47.57 While there are precedents for requiring agencies to conduct PIAs, the ALRC is not aware of any jurisdiction that requires an organisation to conduct a PIA in relation to new projects or developments. There has been discussion, however, about extending a PIA process to the private sector in the UK. The UK Information Commissioner has proposed that PIAs be introduced 'to ensure public confidence in initiatives and technologies which could otherwise accelerate the growth of a surveillance society'.[94] The UK Information Commissioner argued that the introduction of PIAs would 'ensure organisations set out how they will minimise the threat to privacy and address all the risks of new surveillance arrangements before their implementation'.[95] As noted above, this process has commenced with the establishment of a PIA handbook, encouraging organisations to undertake PIAs voluntarily as part of their business management and risk assessment processes.

Submissions and consultations

47.58 In DP 72, the ALRC identified support in submissions and consultations for the process and benefits of conducting a PIA. There was disagreement, however, about

---

90 *E-Government Act of 2002* 2458 Stat 803 (US) s 208.

91 United Kingdom Government Information Commissioner's Office *Privacy Impact Assessment Handbook* (2007).

92 Ibid.

93 Ibid.

94 United Kingdom Government Information Commissioner's Office, 'Information Commissioner Calls for New Privacy Safeguards to Protect against the Surveillance Society' (Press Release, 1 May 2007).

95 Ibid.

whether the process should be mandatory or voluntary, and whether it should apply to organisations as well as agencies. In particular, there was a reluctance to introduce a mandatory PIA process, for fear that it would increase the regulatory burden and make a PIA a 'box-ticking exercise', rather than a genuine assessment of privacy risks.

47.59 In terms of the process of conducting a PIA, stakeholders generally agreed that the PIA should be undertaken by the relevant agency or organisation itself, as responsibility to ensure that a project complies with the *Privacy Act* ultimately rests with the agency or organisation undertaking the project. It was suggested, however, that the OPC should have some oversight or monitoring role.

47.60 In DP 72, the ALRC expressed the view that the PIA process should have a statutory underpinning in the *Privacy Act*. The ALRC suggested that this could either take the form of amending the Act to include a requirement to prepare a PIA for proposed projects and developments that have a significant impact on the handling of personal information, or the current voluntary approach could continue but the Commissioner also given a power to direct that a PIA be undertaken.

47.61 Having regard to the fact that the voluntary process had been in place for agencies for just over a year, and conscious of the regulatory burden that a mandatory requirement would impose, the ALRC proposed that the second option be adopted. That is, that the *Privacy Act* be amended to empower the Privacy Commissioner to direct an agency or organisation to provide to the Commissioner a PIA in relation to a new project or development that the Commissioner considers may have a significant impact on the handling of personal information, and to report to the Minister on any failure to comply with such a direction.[96] The ALRC also proposed that the OPC produce guidelines on the PIA process tailored to the needs of organisations, as organisations were included in the proposed scope of the power.

47.62 The ALRC received a large number of submissions on this proposal. Strong support was received from the Australian Privacy Foundation;[97] and a number of other stakeholders and interest groups also supported the proposal.[98]

47.63 Medicare Australia submitted that agencies should be encouraged to conduct PIAs for new projects and developments, rather than having a PIA process imposed on them. It argued that a mandatory approach could result in the process being seen as an administrative burden, which would lead to agencies 'going through the motions',

---

96 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–4.

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

98 Australian Government Centrelink, *Submission PR 555*, 21 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; P Youngman, *Submission PR 394*, 7 December 2007.

rather than using it as a genuine opportunity to ensure that best privacy practice is built into the project design.[99]

47.64 The Public Interest Advocacy Centre (PIAC) argued that PIAs are a crucial aspect of proactive privacy regulation and that the ALRC's proposal did not go far enough.

> It should be mandatory for agencies and organisations to provide and publish PIAs for all new projects and developments that have the potential to significantly impact on privacy. It should not be left up to the Privacy Commissioner to 'direct' that a PIA be carried out. This assumes that the Commissioner will have some advance knowledge of the proposed project or development. It would not be difficult for an agency or organisation to limit publicity and information about new projects or developments, thus circumventing a PIA direction. Indeed, there will often be circumstances in which an agency or organisation seeks to keep the development confidential for business or political reasons. Moreover, if the Commissioner is poorly resourced or giving priority to other functions such as complaint handling, it is not difficult to imagine the function of directing PIAs falling by the wayside.[100]

47.65 The OPC supported PIAs being undertaken for agency projects that have a significant impact on the handling of personal information, but did not support an explicit power to direct either agencies or organisations to undertake a PIA. In particular, in relation to organisations:

> The Office considers that imposing a requirement that PIAs be conducted by organisations at the direction of the Privacy Commissioner may result in a perception of privacy being a burden imposed on an organisation by the regulator, rather than adopted and built in by the organisation in an effort to ensure best practice and consumer confidence. This appears to be a departure from the current model which is underpinned by the concept that organisations are best equipped to undertake risk analysis of their own business, and determine how the principle based law can best be applied in their circumstances.[101]

47.66 A number of private sector organisations opposed the proposal.[102] Most took the view that any power given to the OPC to direct that a PIA be undertaken would be an additional compliance burden, and add increased costs to projects and developments.[103]

---

99 Medicare Australia, *Submission PR 534,* 21 December 2007.

100 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

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

102 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; Confidential, *Submission PR 536,* 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; Financial Planning Association of Australia, *Submission PR 496,* 19 December 2007; Insurance Council of Australia, *Submission PR 485,* 18 December 2007; Microsoft Asia Pacific, *Submission PR 463,* 12 December 2007; Telstra Corporation Limited, *Submission PR 459,* 11 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

103 Australasian Compliance Institute, *Submission PR 419,* 7 December 2007;

47.67 This view was shared by the Department of Broadband, Communications and the Digital Economy, which submitted that the proposal could have a significant impact on an agency's capability to implement quickly new Government policies, and on the resources available to do so. It argued that the proposal also would place a significant compliance burden on private organisations.[104]

47.68 A number of stakeholders took the view that the proposal was inconsistent with principles-based regulation.[105] Telstra argued that organisations should be free to determine how to comply with the *Privacy Act*.

> It is appropriate for the OPC to issue guidelines on good practice and preparation of PIAs, but the Privacy Commissioner should not be directing how to manage compliance, whether organisations undertake PIAs, or how those PIAs should be carried out. Ultimately, if an organisation fails to comply with the *Privacy Act*, it will be accountable as there are effective enforcement tools available to the Privacy Commissioner.[106]

47.69 The Australasian Compliance Institute expressed the view that the OPC could achieve the same result through releasing guidelines in relation to when PIAs should be undertaken. It argued that, given the OPC is unlikely to find out about projects or developments until they are well advanced, the value in the OPC being able to direct that a PIA be undertaken at that point in time is questionable, particularly given the cost and time delay that such assessments may generate.[107]

47.70 The National Transport Commission 'did not disagree' with the proposal, but expressed concern that the proposal could duplicate what already occurs as part of the regulatory impact statement (RIS) process. Development of an RIS by agencies is mandatory for all reviews of existing regulation and proposals for new or amended regulation.[108] In reforms that have a privacy dimension, the department, agency, or body preparing the RIS is required to canvass such issues with relevant stakeholders, which would include the applicable state and federal Privacy Commissioner, and would have to incorporate their views and any submissions they make in the RIS.[109]

---

104 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

105 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

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

107 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

108 All Commonwealth policy proposals that have a significant impact on business and individuals or the economy (whether in the form of compliance costs or other impacts) require the preparation of an RIS. Before consideration of the proposal by Cabinet or the relevant Minister, the RIS must be considered by the Office of Best Practice Regulation: see Australian Government Office of Best Practice Regulation, *Role of the OBPR* <www.obpr.gov.au/role.html> at 15 May 2008.

109 National Transport Commission, *Submission PR 416*, 7 December 2007.

ALRC's view

47.71 Agencies and organisations should be encouraged to conduct PIAs for new projects and developments, and the OPC should educate agencies and organisations about the value of PIAs and the process involved in conducting a PIA.[110] With the exception of Canada, no other jurisdiction has mandatory PIAs. In the UK and New Zealand, the current approach is to encourage the voluntary use of PIAs and provide clear guidance as to their benefits.

47.72 This encouragement and education should be supported by a power vested in the Privacy Commissioner to direct agencies to prepare a PIA in relation to projects that may have a significant impact on the handling of personal information, and for the Commissioner to report to the Minister on non-compliance with such a direction.

47.73 For the reasons outlined below, however, the power to direct the preparation of a PIA should be limited to agencies and not apply to organisations. In relation to agencies, this proposal was supported by a number of large government departments, such as Centrelink, Medicare and the Department of Human Services.[111]

47.74 A power to direct the preparation of a PIA should not place as large a compliance burden on agencies as a mandatory scheme, but rather strengthen the existing voluntary regime. It is envisaged that the power to direct a PIA would be used primarily in two circumstances. First, it could be used where the OPC currently recommends that a PIA be undertaken, as part of its policy advice on a proposal or bill. Rather than being limited to 'recommending', the OPC would have the ability to direct, where appropriate, the agency to prepare the PIA. Secondly, it could be used where there has been some publicity about a project or development, or a complaint, inquiry or tip-off, and the OPC concludes that the project or development may have a significant impact on the handling of personal information.

47.75 Monitoring compliance with a direction to prepare a PIA should be less onerous and more manageable than monitoring compliance with a mandatory scheme, and the power to report non-compliance to the Minister should have a valuable deterrent effect. As part of the Commissioner's auditing functions, the Commissioner also would be able to assess the extent to which an agency or organisation complies with the voluntary PIA guide. This may prompt the Commissioner to keep a closer watch on agencies or organisations that do not appear to be conducting PIAs where

---

110 In relation to terminology, the ALRC continues to adopt the definition of 'project' in the PIA Guide, where it is used to refer to any proposal, review, system, database, program, application, service or initiative that includes the handling of personal information: Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 3. The ALRC notes that a project could be a new development or a new policy proposal, and a project may be implemented by legislation or administratively.

111 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

appropriate.[112] If a project raised serious privacy concerns, the Commissioner could apply to the Federal Court or the Federal Magistrates Court for an injunction to stop the agency from implementing the project, pending the preparation of the PIA and the review of that assessment by the OPC.[113]

47.76 The relevant agency should prepare (or obtain) the PIA, as compliance with the Act is its responsibility, and the project or development is its concern. The OPC should continue to review and provide guidance and advice on the PIA process, to ensure it addresses and resolves adequately privacy issues.[114]

47.77 The power to direct a PIA should not, however, replace the role of the existing voluntary guidelines. These guidelines strongly encourage PIAs to be produced in certain circumstances, and agencies should not wait for a direction from the OPC where they believe a PIA is warranted. The power to direct should be required only as a last resort, where the Commissioner feels that a PIA is necessary and is not being considered by the agency.

47.78 As noted above, PIAs are most effective when they are undertaken at the start of a project. Some stakeholders suggested that the Commissioner will not be in a position to know that a project, which requires a PIA, has commenced. Even if a PIA was mandatory, however, there would be no way to ensure that it was being conducted at the commencement of a project, unless it was required to be provided to the OPC. Such a requirement would have considerable resource implications. One way to ameliorate these concerns is to encourage more informal dialogue between agencies and the OPC through the Privacy Contact Officers network, so that the OPC is aware of major projects that are being proposed that may require a PIA.

47.79 The ALRC notes the concern that undertaking a PIA may duplicate the RIS process. While some agencies may consider privacy issues as part of an RIS, it does not appear from submissions and consultations that this is a universal practice. Furthermore, not every project which has a significant impact on the handling of personal information will require an RIS. The purpose of an RIS is to ensure that government policymaking does not lead to unnecessary regulation and compliance burdens. As part of the process, policymakers identify the options (regulatory and non-regulatory) for achieving the desired objective of the policy and assess of the impact (costs and benefits) on consumers, business, government, the environment and the community of each option.[115] The role of a PIA is quite different in that it describes the

---

112 The OPC already monitors compliance with voluntary guidelines, such as the Data-Matching Guidelines, even though they are not binding. See Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 9.

113 *Privacy Act 1988* (Cth) s 98.

114 This is consistent with the approach recommended in B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61.

115 Australian Government Office of Best Practice Regulation *Best Practice Regulation Handbook* (2006), Part 3.

personal information flows in a project and analyses the possible impact on privacy of those flows, and is not conducted from a cost/benefit perspective. The ALRC, therefore, is of the view that any work done in completion of an RIS could assist the PIA process or vice versa, but the completion of both may be necessary in some instances.

47.80 Private sector stakeholders did not support the proposal to allow the OPC to direct organisations that a PIA must be undertaken where the Commissioner considers that a project may have a significant impact on the handling of personal information. While many new projects or developments undertaken by organisations would benefit from being subject to PIAs to ensure that the privacy risks are assessed and adequately managed, this may also result in a significant compliance burden. If the recommendation to remove the small business exemption from the *Privacy Act* is implemented,[116] there will already be some additional compliance costs for small businesses.

47.81 There are different policy considerations which favour a power to direct agencies to complete a PIA. PIAs serve an important function in the public sector, because individuals are able to exercise less control over their own personal information. In a commercial context, parties are free to enter and withdraw from transactions according to their own interests.[117]

47.82 The strongest argument in favour of not directing organisations to undertake a PIA is that the OPC has not yet issued voluntary guidelines for private sector PIAs. Given that the private sector has not yet been given the opportunity to adopt the voluntary guidelines, the ALRC does not recommend that the Privacy Commissioner be empowered to direct organisations to undertake a PIA.

47.83 Instead, and consistently with the approach taken to agency PIAs, the ALRC recommends that the OPC produce a PIA guide tailored to the needs of organisations. Such a guide should help to educate organisations on the value of a PIA, the process involved, and the assistance that the OPC can give. The OPC also should include guidance in the respective PIA guides on what constitutes a 'significant impact on the handling of personal information'. These circumstances could draw on the examples put forward by Blair Stewart,[118] including where: the project or development involves a new technology or the convergence of an existing technology; the use of a known technology in a new privacy-intrusive circumstance; or a major endeavour or change in practice that has obvious privacy risks.[119]

---

116 Rec 39–1.

117 See S Bloomfield, 'The Role of the Privacy Impact Assessment' (Paper presented at Managing Government Information: 2nd Annual Forum, Ottawa, 10 March 2004).

118 Assistant Commissioner (Policy), Office of the Privacy Commissioner New Zealand.

119 See B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61.

47.84 Once the voluntary guidelines are in place, a review should be undertaken in five years from the commencement of the amended *Privacy Act* to assess whether the power in Recommendation 47–4 should be extended to include organisations.[120]

Recommendation 47–4 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) direct an agency to provide to the Privacy Commissioner 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; and

(b) report to the ministers responsible for the agency and for administering the *Privacy Act* on the agency's failure to comply with such a direction.

Recommendation 47–5 The Office of the Privacy Commissioner should develop and publish Privacy Impact Assessment Guidelines tailored to the needs of organisations. A review should be undertaken in five years from the commencement of the amended *Privacy Act* to assess whether the power in Recommendation 47–4 should be extended to include organisations.

Compliance powers

47.85 Regulatory theorists suggest that a critical part of ensuring compliance with a regulatory regime is to monitor and enforce implementation of the regime by the regulated entities.[121] The Commissioner's functions in monitoring compliance with the *Privacy Act* include: conducting audits and examining records; receiving, investigating and resolving privacy complaints; enforcing the Act through determinations, injunctions and federal court proceedings; and determining that certain acts or practices will not be taken to breach the Act where there is a substantial public interest in so doing.

47.86 The Commissioner's complaint-handling and enforcement powers are discussed in Chapters 49 and 50. This part of the chapter focuses on the Commissioner's auditing functions, including self-auditing and PIDs.

120 See also Recs 3–6 and 54–8.

121 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 535; F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341.

Audit functions

Background

47.87 The Commissioner has a number of functions under the *Privacy Act* to audit compliance. The OPC describes an audit as 'a snapshot of personal information handling practices in relation to an agency or organisation program at a certain time and in a particular location'.[122] An audit involves a systematic inspection and review of an agency or organisation, to obtain evidence to enable the Commissioner to assess the extent to which records are maintained in accordance with various provisions of the Act.[123] The 'spot-audit' and examination functions conferred on the Commissioner are divided among the IPPs,[124] TFN information,[125] and credit reporting provisions.[126]

47.88 The number of audits carried out each year by the OPC has 'varied over the life of the *Privacy Act* depending on the nature of privacy complaints and other priorities of the Office'.[127] The OPC notes, in its 2006–07 Annual Report, that consistent with the approach taken since 2002–03, the OPC mainly undertook audits where it received specific funding to so do. With the clearing of the backlog of complaints in late 2007, the OPC expects to expand its audit program in 2008.[128]

Audits of organisations

47.89 Organisations are subject to audit by the Commissioner under functions associated with the TFN and credit reporting provisions, as discussed above. There is no general power to 'spot audit' the privacy compliance of organisations. If an organisation requests it, however, the Commissioner can examine the records of personal information maintained by the organisation, for the purpose of ascertaining whether the records are maintained in compliance with either an approved privacy code or the NPPs, as applicable.[129] As at the date of the OPC Review, the Commissioner had not conducted any audits under this power.[130]

---

122 Office of the Privacy Commissioner, *Audit Information* (2007) <www.privacy.gov.au/government/audits/index.html> at 15 May 2008.

123 Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 5. See also Office of the Privacy Commissioner, *Privacy Audit Manual—Part II (Tax File Number Guidelines)* (1995); Office of the Privacy Commissioner, *Privacy Audit Manual—Part III (Credit Information)* (1995).

124 *Privacy Act 1988* (Cth) ss 27(1)(h), 27(1)(h).

125 Ibid s 28(1)(d), 28(1)(e), 28(1)(h).

126 Ibid s 28A(1)(g), 28A(1)(j). Note, the Commissioner also has a monitoring role under the *Telecommunications Act 1997* (Cth), which is discussed further in Part J.

127 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 60.

128 Ibid, 60.

129 *Privacy Act 1988* (Cth) s 27(3).

130 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 157.

Previous inquiries

47.90 Several stakeholders making submissions to the OPC Review and Senate Committee privacy inquiry submitted that the NPPs should be amended to confer an audit power on the Commissioner.[131] One participant in the OPC Review commented that if the Commissioner had audit powers, 'we might be able to convince our boards to comply [with the *Privacy Act*]'.[132] Others expressed the view that an extended audit power is necessary to maintain public confidence in the Commissioner's role.[133]

47.91 The OPC Review did not recommend, however, that the Commissioner be given the power to audit organisations. While recognising that a private sector audit power may increase community confidence in the efficacy of the *Privacy Act* and give the OPC additional power to identify systemic issues and to monitor responses, the OPC concluded that it would have resource implications and may be a more appropriate role for private consultants to perform.[134] The OPC Review recommended instead that it would 'consider promoting privacy audits' by organisations, such as by providing information on the value of auditing as evidence of compliance in the event of complaints, and by developing and providing privacy audit training.[135] In contrast, the Senate Committee privacy inquiry urged the introduction of OPC private sector auditing powers.[136]

Private sector audits in other jurisdictions

47.92 The Canadian Privacy Commissioner has power to conduct audits of private sector organisations under the *Personal Information Protection and Electronic Documents Act 1985* (Canada).[137] This Act provides that the Canadian Privacy Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organisation if the Commissioner has reasonable grounds to believe that the organisation is contravening particular provisions of the Act.[138]

47.93 The UK Information Commissioner's power to conduct audits on private sector organisations has a limitation, similar to that of the OPC—it can only be done with the

---

131 See Ibid, 145; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.35], [6.39].

132 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 133.

133 Ibid, 145.

134 Ibid, 157.

135 Ibid, rec 39.

136 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.56].

137 The Canadian Privacy Commissioner also has power to conduct audits on government bodies: *Privacy Act* RS 1985, c P-21 (Canada) ss 37–39.

138 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada). Guidance on the circumstances that may lead to an audit is provided in Office of the Privacy Commissioner of Canada, *A Guide for Businesses and Organizations: Your Privacy Responsibilities—Canada's Personal Information Protection and Electronic Documents Act* (2004) <www.privcom.gc.ca/information/guide_e.asp> at 14 May 2008, 25.

organisation's consent.[139] The UK Information Commissioner has consistently called for stronger powers to allow his Office to carry out inspections and audits of organisations without the organisation's consent, arguing that the requirement for consent 'fetters' the power to conduct audits and inspections and 'limits proactive oversight and the deterrent effect of possible inspection in areas where there may be real risks to compliance'.[140]

Submissions and consultations

47.94 In DP 72, the ALRC identified support in submissions and consultations for the Commissioner's existing audit powers. Stakeholders also generally supported introducing a private sector audit power, although there were those who favoured extending the Commissioner's power without limitation (similar to the power to audit agencies) and those in favour of extending it with some qualification—for example, restricting its use to where there is evidence of some widespread or systemic issues in the organisation or industry.[141]

47.95 In DP 72, the ALRC proposed that the audit power be extended to the private sector, without qualifying the power.[142]

47.96 There was support for the proposal from a number of stakeholders.[143] The Australian Lawyers Alliance, for example, suggested that the fact that the Commissioner has not conducted any audits to date demonstrates the current regime has not been highly successful.[144]

47.97 A number of organisations, however, opposed the proposal on the basis that a general audit power was unnecessary, would create a compliance burden and is inconsistent with an outcomes-based regulatory approach.[145] Stakeholders from the financial services industry noted that their businesses already are subject to a number of notification, self-audit or audit requirements from other regulators, such as the

---

139 *Data Protection Act 1998* (UK) s 51(7).

140 United Kingdom Government Information Commissioner's Office, *Evidence Submitted to the Home Affairs Committee Inquiry into 'The Surveillance Society?'* 23 April 2007, 7. These calls were also made following the loss of over 25 million records by Her Majesty's Revenue and Customs Service in November 2007. See, eg, R Blakely, 'Data "Fiasco" Leads to Call for Law Changes', *Times Online* (Online), 20 November 2007, <business.timesonline.co.uk>.

141 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Ch 44.

142 Ibid, Proposal 44–6.

143 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Lawyers Alliance, *Submission PR 528*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 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; P Youngman, *Submission PR 394*, 7 December 2007.

144 Australian Lawyers Alliance, *Submission PR 528*, 21 December 2007.

145 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

Australian Securities and Investments Commission (ASIC), the Australian Prudential Regulation Authority, the Australian Transaction Reports and Analysis Centre and state and territory fair trading agencies.[146] It was argued that the resources required to comply with an audit power would be high, and disproportionate to the likely benefits to consumers. Avant submitted that 'in light of a system to hear complaints about breaches of the *Privacy Act* having spot-audits is unnecessary over regulation'.[147]

47.98 A large number of stakeholders were supportive of introducing a qualified audit power.[148] The OPC recommended the introduction of a qualified audit power (expanding on its 'own motion' investigation functions) to allow the Office to audit organisations where the Privacy Commissioner had reasonable grounds to believe that the organisation was engaging in practices that:

- posed new and significant risks to personal information they hold; or
- contravened the privacy principles in the Act or a commitment made in resolution to a complaint or own motion investigation.

47.99 In the OPC's view:

> this approach allows pro-active assistance to be provided to organisations seeking to introduce new technologies or projects, and to have the power to appropriately react when the Office is made aware of situations where particular risks or practices of concern have been identified such as significant systemic breaches.[149]

47.100 The OPC also suggested that use of the word 'audit' may have inherent negative connotations—characterising the relationship between the OPC and the organisation as that of 'police officer and suspect'. In the OPC's view, this could undermine efforts to encourage organisations to recognise the inherent value in good privacy practice and the role of the OPC in assisting organisations in this regard. The OPC suggested that the use of the term 'privacy performance assessment' might reflect this approach better.[150]

47.101 Some stakeholders did not support audits of organisations in principle, but argued that if they were to be used, then this should be only where the OPC has

---

146 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

147 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

148 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Financial Planning Association of Australia, *Submission PR 496*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

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

150 Ibid.

reasonable grounds to suspect that an organisation is not complying with the *Privacy Act*.[151] In the view of Australian Unity, however, the OPC's own motion investigation powers would better serve the purpose of investigating an organisation where a real suspicion about compliance existed.[152] Telstra also expressed the concern that a 'spot audit' power

> may complicate the overall enforcement approach if the Privacy Commissioner could undertake an audit to address situations where there is a reasonable belief that the organisation is engaging in non-compliant acts or practices. There is a real risk that a spot audit would compromise own motion investigations and create a lot of uncertainty for organisations around the purposes or function of any audit by the Privacy Commissioner.[153]

47.102 The Australasian Compliance Institute stated that, if the OPC were granted an 'own motion' power, then it would support the audit power being used as an educative tool to assist organisations to identify areas for improvement within their privacy compliance frameworks.[154] The Department of Human Services, while giving support to the proposal, agreed that audits should be focused on education and prevention, rather than the imposition of penalties.[155]

ALRC's view

47.103 The OPC's audit functions are an important part of its compliance activities. The power to conduct audits is one of the few proactive regulatory tools vested in the OPC, in that it allows the Commissioner to monitor an agency or organisation's compliance with the *Privacy Act* before, and in the absence of, evidence of non-compliance, with the aim of preventing such non-compliance occurring in the future. It also allows the Commissioner to identify systemic issues and bring about systemic change, and to use information gathered in an audit to target educational materials and programs.[156]

47.104 The ALRC supports the OPC's suggestion that audits should be referred to as 'Privacy Performance Assessments' (PPAs) to emphasise the educational and non-confrontational nature of the process.

---

151 Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007;

152 Australian Unity Group, *Submission PR 381*, 6 December 2007.

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

154 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

155 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

156 See Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 50. See also Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 60.

Own motion investigations

47.105 It is important to maintain a clear distinction between the Commissioner's PPA functions under the Act, which are educative and preventative, and the power to conduct an own motion investigation.

47.106 Where the OPC has a reasonable belief that an organisation is engaging in practices that contravene the privacy principles in the Act, then the appropriate power to investigate such conduct is the own motion investigation power. The point of the own motion investigation power is to allow the Commissioner to investigate an act or practice that may be an interference with privacy of an individual.[157] It is not appropriate for the Commissioner to respond to such circumstances by undertaking a process with a purely educational focus. In addition, the distinction between an own motion investigation and a PPA will be much clearer if the ALRC's recommended compliance order power is implemented, which would empower the Commissioner to issue an order following an own motion investigation.[158] These issues are discussed further in Chapter 50.

47.107 Where the Commissioner is of the view that the act or practice that is breaching the settlement conditions is also an interference with privacy—where, for example, an organisation has continued a practice that the Commissioner has previously investigated and found to be in breach of the *Privacy Act*—then it would be more appropriate and effective to launch a new own motion investigation, rather than to conduct a PPA, so that the Commissioner can issue a compliance order (which can be enforced in the Federal Court), or an enforcement action to be commenced in the Federal Court, if a determination or compliance notice has already been issued.

Audit function

47.108 In relation to private sector audits, there is some consensus among stakeholders that the Privacy Commissioner should have a power to conduct a PPA of organisations to assess compliance with the NPPs. The difference of opinion arises as to when the Commissioner should be able to exercise the power, and, in particular, whether the Commissioner should have a wide or a qualified power.

47.109 The real value of PPAs lies in their proactive nature—they can be used to take a snapshot of the level of compliance in an agency or organisation or across an industry. The presence of an audit power can act as an important preventative measure, as 'the existence of the audit functions and programs encourages organisations subject to the Act to take compliance seriously'.[159]

---

157 See s 40(2).

158 Rec 50–1.

159 See Office of the Privacy Commissioner, *Audit Information* (2007) <www.privacy.gov.au/government/audits/index.html> at 15 May 2008.

47.110 The Commissioner should be empowered, therefore, to conduct a PPA on the levels of compliance in organisations more generally, as he or she is currently empowered to do in relation to agencies.

47.111 In addition, where the Commissioner is concerned that the organisation is engaging in practices that pose new and significant risks, but does not think that the acts or practices currently constitute an interference with privacy, then the Commissioner could, and should, undertake a PPA. Even where the risk identified may be speculative and may not have eventuated, it would be appropriate to use the PPA power, as such a power has an educational focus.

47.112 PPAs also could have a role to play following a complaint settlement or determination, or the issuance of a compliance notice.[160] In particular, it may be valuable for the Commissioner to undertake pre-emptive 'spot' PPAs to assess whether the organisation is abiding by the terms of the settlement, determination or compliance notice—or to require the organisations themselves to undertake such audits. This is analogous to an undertaking under s 87B of the *Trade Practices Act 1974* (Cth), which may include agreement by the company to have its compliance program independently audited for a number of years and provide the audit report to the Australian Competition and Consumer Commission (ACCC).[161]

47.113 The ALRC's approach is consistent with the current position of audits on the compliance spectrum—that is, they are considered primarily educative and there are no penalties attached to a poor privacy audit (unless there is some evidence of deliberate wrongdoing).[162]

47.114 The ALRC does not agree that PPAs are inconsistent with principles-based regulation. A PPA does not involve the Commissioner mandating the steps that an organisation must take to comply with the Act. Rather, the Commissioner is assessing whether the steps the organisation has decided to take meet the objectives of the principles.

Audit manuals

47.115 If the Commissioner's audit function were expanded to include private sector audits, it would be valuable for the OPC to develop an audit manual for organisations (or amend the existing IPP Manual) to provide further detail on the processes involved in an audit. In addition, the audit manuals should clarify when the results of an audit will be used in an educative and collaborative manner, and when they may lead to

---

160 Rec 50–1.

161 Australian Competition and Consumer Commissioner, *Section 87B of the Trade Practices Act: A Guideline on the Australian Competition and Consumer Commission's Use of Enforceable Undertakings* (1999), 7.

162 The TFN Manual explains that, if any evidence of deliberate breaches of the Guidelines are detected by the auditors, the matter will be referred to the relevant authority for consideration of further action: Office of the Privacy Commissioner, *Privacy Audit Manual—Part II (Tax File Number Guidelines)* (1995), 4.

sanctions. Audit manuals should be updated to reflect the OPC's current expectations as to the levels of compliance to be achieved by agencies and organisations.[163]

Consolidating audit functions

47.116 Consistently with the ALRC's recommendation that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity,[164] the audit functions of the Commissioner should be consolidated. Given the ALRC's recommendation to introduce Unified Privacy Principles (UPPs),[165] audit functions for agencies and organisations could be combined and could include TFN and credit reporting auditing. References to agencies or organisations would include agencies or organisations in their capacity as TFN recipients and as credit providers or credit reporting agencies, as applicable.

Recommendation 47–6 The *Privacy Act* should be amended to empower the Privacy Commissioner to conduct 'Privacy Performance Assessments' of the records of personal information maintained by organisations for the purpose of ascertaining whether the records are maintained according to the model Unified Privacy Principles, privacy regulations, rules and any privacy code that binds the organisation.

Self-auditing

Background

47.117 A possible alternative or addition to the Commissioner's power to conduct PPAs would be the imposition of a requirement on agencies or organisations to undertake self-auditing.[166] The *Corporations Act 2001* (Cth) model of financial reporting and audits was suggested as a possible model. That model includes an obligation on corporations to self-audit, to report periodically to ASIC, and to be subject to audit by ASIC. By analogy, organisations subject to the federal privacy regime could be required to self-audit privacy compliance and, if requested by the

---

163 The ALRC notes that the manuals reflect the Commissioner's expectations at the time the Manuals were published, which may now be outdated. For example, the Credit Reporting Manual sets out that, as credit reporting provisions have only been in force since 1992, the 'Commissioner has taken the view that credit providers should be given the benefit of the doubt where instances of breach are detected. In any case only in clearly culpable circumstances would further action be taken'. See Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), [1.6.1]–[1.6.2].

164 Rec 5–2.

165 Rec 18–2.

166 M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006. See also M Crompton, 'Respecting People, Their Individuality and Their Personal Information: The Key to Connected Government, Now and in the Future' (Paper presented at Public Services Summit, Stockholm, 9 December 2005). See also Baycorp Advantage, *Consultation PC 2*, Sydney, 24 February 2006.

OPC, report to the Commissioner on their compliance.[167] The Commissioner could then conduct a PPA on such organisations as the Commissioner chooses, without being required to assess every organisation.

47.118 There is some movement towards self-auditing for privacy in the United States. While some regimes, particularly those relating to the private sector, 'do not explicitly require the formal conduct and report of an audit, auditing is generally necessary in order to be in full compliance'.[168]

Submissions and consultations

47.119 In DP 72, the ALRC identified both support and opposition from stakeholders for requiring self-auditing for privacy compliance.[169]

47.120 While the ALRC did not propose that a self-audit requirement be introduced into the Act, it recognises that in some situations the UPPs may require a self-audit in order to be in full compliance with the principles. Prior to the *Privacy Act* being redrafted however, it was thought that instituting a self-audit requirement would be premature.

47.121 Before such a requirement can be considered, there needs to be uniformity in the privacy regimes across Australia.[170] The ALRC was also concerned that a requirement to self-audit may improve levels of compliance only if results are reported and the OPC has the time and resources to monitor self-audit reports produced and conduct spot audits to verify the self-auditing process. This would place a large compliance burden on agencies and organisations, and require significant use of OPC resources. It would also be particularly onerous for small businesses, if the ALRC's recommendation to abolish the small business exemption were implemented.[171]

47.122 The ALRC did not receive further comments in response to DP 72 in relation to this issue.

ALRC's view

47.123 For the reasons outlined above, the ALRC has concluded that agencies and organisations should not be required to self-audit and report on privacy compliance.[172]

---

167 A stakeholder to the Senate Committee privacy inquiry suggested a 'self-audit-self-regulatory process' as a more efficient way to deal with complaints: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.21].

168 C Easter, 'Auditing for Privacy' (2006) 2 *I/S: A Journal of Law and Policy for the Information Society* 879, 880.

169 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [44.101]–[44.111].

170 In Ch 3, the ALRC makes several recommendations in this regard.

171 Rec 35–1.

172 This view was supported in submissions: Law Council of Australia, *Submission PR 527*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

The OPC should continue, however, to educate agencies and organisations on the value of self-auditing, including to ensure compliance with the recommended 'Openness' principle.[173] The OPC also should clarify situations where it will regard a self-audit policy as a reasonable step to take to ensure the protection of personal information held, in compliance with the recommended 'Data Security' principle.[174]

Functions under other Acts

Background

47.124 In addition to the functions enumerated in the *Privacy Act*, the Commissioner has functions under other legislation.[175] In summary, these functions are to:

- Issue the *Data-matching Program (Assistance and Tax) Guidelines* and to investigate an act or practice that may breach the Guidelines or Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth).[176]

- Issue the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* and to investigate an act or practice that may breach the guidelines.[177]

- Monitor compliance with the record-keeping requirements under Part 13 of the *Telecommunications Act 1997* (Cth).[178] The Commissioner also must be consulted about industry codes and standards that deal with privacy issues pursuant to Part 6 of the *Telecommunications Act*,[179] and must be consulted before the Australian Communications and Media Authority enforces an industry code relating to a matter dealt with by the NPPs or an approved privacy code.[180]

---

173 In particular, self-auditing can help agencies and organisations ensure that they have an adequate Privacy Policy in place. See also Ch 24. A similar suggestion was made in Veda Advantage, *Submission PR 163*, 31 January 2007.

174 See Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

175 These functions are set out in more detail in Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [6.66]–[6.75].

176 Issued pursuant to *Privacy Act 1988* (Cth) s 27(1)(p) and *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 12(2). These replaced the interim guidelines set out in *Privacy Act 1988* (Cth) sch 2. The current guidelines came into effect on 14 April 1997.

177 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997), 2–3.

178 *Telecommunications Act 1997* (Cth) s 309.

179 Ibid ss 117(1)(j), 117(1)(k), 118, 134. In 2006–07, the Privacy Commissioner was consulted on eight Australian Communications Industry Forum codes developed pursuant to the *Telecommunications Act 1997* (Cth): Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [1.7.3].

180 *Telecommunications Act 1997* (Cth) ss 121, 122.

- Investigate and determine complaints about breaches of the spent convictions scheme in Part VIIC of the *Crimes Act* and to assess applications for complete or partial exclusions from the requirements of the scheme.[181]

Submissions and consultations

47.125 In DP 72, the ALRC identified support in submissions and consultations for consolidating all the Privacy Commissioner's functions in the *Privacy Act*, including where the functions are presently under other legislation.[182] While the ALRC agreed that listing all functions in the *Privacy Act* would be ideal, it acknowledged that it may not be practical to expect that the *Privacy Act* would be amended each time the Commissioner was given a new function under another piece of legislation. Instead, the ALRC proposed that the OPC maintain and publish on its website a list of all the Privacy Commissioner's functions, including those functions that arise under other legislation.[183]

47.126 The proposal received almost unanimous support from stakeholders.[184] The Cyberspace Law and Policy Centre argued that all of the Commissioner's functions should be located or relocated, or if appropriate repeated, in the *Privacy Act*. It argued that any other legislation to which a function relates should contain an explicit cross-reference to the Commissioner's role and the *Privacy Act* function.[185]

ALRC's view

47.127 Consistently with the ALRC's recommendation that the *Privacy Act* should be redrafted to achieve greater logical consistency, simplicity and clarity,[186] it would be of assistance to stakeholders if the OPC listed its functions on the OPC's website, where the function arises in the *Privacy Act* and under other legislation. While the ALRC agrees that it would be preferable for the *Privacy Act* to contain a complete list of the Commissioner's functions it would not be practical for the *Privacy Act* to be amended each time the Commissioner was given a new function.

---

181 *Crimes Act 1914* (Cth) ss 85ZZ, 85ZZC.

182 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; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007. It was also suggested that the Commissioner's functions be listed in a separate schedule to the Act: Privacy NSW, *Submission PR 193*, 15 February 2007.

183 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–7.

184 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

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

186 Rec 5–2.

Recommendation 47–7 The Office of the Privacy Commissioner should publish and maintain on its website a list of all the Privacy Commissioner's functions, including those functions that arise under other legislation.

Public interest determinations

Background

47.128 The Commissioner has the power to make a determination that an act or practice of an agency or organisation, which may otherwise breach an IPP, NPP or approved privacy code, should be regarded as not breaching that principle or privacy code while the determination is in force. Such a determination is called a 'public interest determination' (PID) and is issued under Part VI of the *Privacy Act*.[187]

Nature of determinations

47.129 A PID can be made if the public interest in an agency or organisation doing an act or engaging in a practice which breaches or may breach an applicable IPP, NPP or code provision, outweighs *to a substantial degree* the public interest in adhering to the IPP, NPP, or code provision.[188] A PID made by the Commissioner in relation to organisations (but not agencies) can be given general effect so that it covers all organisations in respect of that act or practice.[189]

47.130 The *Privacy Act* sets out a detailed process for receiving and applying for, consulting on, and issuing a PID. The OPC has issued non-binding guidelines to assist those considering or making applications for a PID,[190] and 'strongly encourages' agencies and organisations to discuss matters with the OPC before making an application.[191]

Temporary public interest determinations

47.131 The Commissioner also has the power to issue a temporary public interest determination (TPID). A TPID has the same effect as a PID but is limited in duration to a maximum of 12 months.[192] The Commissioner can make a TPID in relation to an

---

187 There are similar instruments in other Australian jurisdictions: see *Information Act 2002* (NT) s 81; *Privacy and Personal Information Protection Act 1998* (NSW) s 41. As at April 2008, there were 10 public interest determinations registered, dated from September 1989 with the most recent determination dated December 2007. There are no current temporary public interest determinations: Office of the Privacy Commissioner, *Public Interest Determinations* <www.privacy.gov.au/act/publicinterest/index.html> at 15 May 2008.

188 *Privacy Act 1988* (Cth) s 72(1)–(2). Emphasis added.

189 Ibid s 72(4).

190 Office of the Federal Privacy Commissioner, *Public Interest Determination Procedure Guidelines* (2002).

191 See the Office of the Privacy Commissioner, *Public Interest Determinations* <www.privacy.gov.au/act/publicinterest/index.html> at 15 May 2008.

192 *Privacy Act 1988* (Cth) ss 80A(3)(a), 80B.

act or practice of an agency or organisation, that is the subject of an application for a standard PID, where the application raises issues that require an urgent decision.[193] The Commissioner can give a TPID in respect of an act or practice of an organisation general effect, so that it applies to other organisations.[194]

Discussion Paper proposal

47.132 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the Commissioner's powers to make PIDs and TPIDs were appropriate and administered effectively.[195] Most stakeholders submitted that the powers are appropriate,[196] with the OPC suggesting that they provided 'necessary flexibility' to respond to situations where 'the operation of the high level privacy principles in the *Privacy Act* may be inconsistent with the public interest'.[197]

47.133 The OPC noted, however, that it lacks any discretion under the *Privacy Act* to dismiss an application for a PID or decline to consider it. This means that once an application is made to the OPC, it must embark on the lengthy consultation process set out in the Act. The OPC submitted that 'as such, there is a risk that an application could be made frivolously or vexatiously or where there is clearly no merit and the Commissioner would then be bound to undertake full consideration of the matter'.[198]

47.134 To address the above concerns, and give the OPC greater flexibility in the PID process, the ALRC proposed that the *Privacy Act* should be amended to give the Commissioner discretion to decline to accept an application for a PID where the Commissioner is satisfied that the application is frivolous, vexatious, misconceived or lacking in merit. It was noted that a decision to decline an application would be subject to judicial review.[199]

---

193 Ibid s 80A(1).

194 Ibid s 80B(3)–(4).

195 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–18.

196 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

197 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. Similar comments on the benefits of PIDs were made in Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

198 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

199 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–8.

Submissions and consultations

47.135 The OPC supported the proposal.[200] A number of other agencies and stakeholders also supported the proposal on the basis that it would conserve the OPC's resources.[201]

47.136 Privacy advocates, however, were concerned that the proposal would allow the Privacy Commissioner to dismiss PID applications too readily.[202] The Cyberspace Law and Policy Centre argued that the proposal should be limited to applications:

> where the Commissioner is satisfied that the application is misconceived as to the purposes of public interest determinations, or so lacking in merit as not to be worthy of public consideration.[203]

47.137 PIAC agreed that the Commissioner should have the discretion to refuse to accept applications for PIDs where they are frivolous, misconceived or vexatious, on the basis that these are factors that are usually obvious on the face of an application. In the case of applications lacking in merit, however, it argued that

> it is difficult to see how the Commissioner could make a decision that an application for a public interest determination is 'lacking in merit' without first accepting the application and conducting some preliminary investigations.[204]

ALRC's view

47.138 The ALRC recommends that the *Privacy Act* be amended to give the Privacy Commissioner a discretion to decline to accept an application for a PID where the Commissioner is satisfied that the application is frivolous, vexatious or misconceived. An application that is misconceived may, for example, be an application where the applicant has misunderstood the purpose of a PID or the requirements of the public interest test. This recommendation would set a high standard for dismissing an application outright, and should operate to encourage applicants to discuss their applications with the Commissioner before submitting them, consistent with the PID guidelines. The ALRC also notes that any decision to refuse to accept an application would be subject to judicial review.

47.139 In the case of applications lacking in merit, the ALRC agrees with PIAC's view that some investigation of the issues must be made before such an assessment could be reached. Indeed, the purpose of the consultation process is to assess whether

---

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

201 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

202 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

204 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

the application has merit, in the sense that the public interest in allowing the waiver of compliance outweighs the public interest in upholding the principle. Removal of the words 'lacking in merit' from the original proposal also should meet some of the concerns of privacy advocates that an application may be dismissed too easily by the Commissioner.

47.140 The ALRC does not recommend any reform of the public interest test for the making of a PID or TPID. While the ALRC is recommending that the public interest test used in relation to medical research is changed to 'outweighs' rather than 'substantially outweighs',[205] there are important distinctions between that area and PIDs, which justify keeping the higher test for PIDS. In particular, PIDs have the potential to reduce the protection provided by the privacy principles across broad sectors for significant periods of time. In contrast, approval by a Human Research Ethics Committee is limited to specific research activities for the duration of those activities.

Recommendation 47–8 The *Privacy Act* should be amended to empower the Privacy Commissioner to refuse to accept an application for a Public Interest Determination where the Privacy Commissioner is satisfied that the application is frivolous, vexatious or misconceived.

205 Rec 65–4.

48. Privacy Codes

Contents

Introduction

48.1 In this chapter, the ALRC examines Part IIIAA of the *Privacy Act 1998* (Cth) and the functions vested in the Privacy Commissioner (Commissioner) to approve privacy codes. The chapter discusses amendment of Part IIIA to require that codes operate in addition to the model Unified Privacy Principles (UPPs) and whether there is a need to amend the Act to allow the Commissioner to initiate binding codes.

Part IIIAA Privacy codes

48.2 When bringing organisations within the ambit of the *Privacy Act*, Parliament decided to adopt a co-regulatory approach. It established a framework in which organisations are able to develop specialised codes for the handling of personal information which, when approved, replace the National Privacy Principles (NPPs).[1] This approach was 'designed to allow for flexibility in an organisation's approach to privacy, but at the same time, guarantees consumers that their personal information is subject to minimum standards that are enforceable in law'.[2]

---

1 *Privacy Act 1988* (Cth) s 16A. The code may also cover exempt acts or practices: s 18BAA.

2 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001), 16. See also the comments made in the Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 19.

Commissioner's powers in relation to codes

48.3 Part IIIAA sets out provisions on privacy codes. Generally, the Commissioner has the power to:

- approve privacy codes and variations of approved privacy codes and to revoke those approvals;[3]
- review the operation of approved privacy codes;[4]
- prepare and publish guidelines about the development, approval and variation of privacy codes, and about complaint-handling processes under codes;[5]
- act as an adjudicator under an approved privacy code where the Commissioner has been appointed as the independent adjudicator under that code;[6] and
- consider applications for review of determinations of adjudicators (other than where the Commissioner is the adjudicator) in relation to a complaint.[7]

Requirements for codes

48.4 The content of a code must meet set standards. In particular, a code must incorporate all of the NPPs or set out 'obligations that, overall, are at least the equivalent of all the obligations set out in those Principles'.[8] Subscription to a code is voluntary. Codes must specify the organisations to which they apply, and may be approved even where they apply for a limited period or to a specified activity or industry sector.[9] If a code sets out procedures for making and dealing with complaints, these processes must comply with the Commissioner's guidelines and the prescribed standards.[10]

48.5 Codes are legislative instruments under s 5 of the *Legislative Instruments Act 2003* (Cth). A privacy code approved under Part IIIAA, however, is not subject to disallowance by Parliament.[11] As at April 2008 there were three codes listed on the

---

3 *Privacy Act 1988* (Cth) s 27(1)(aa).
4 Ibid s 27(1)(ad). Review occurs under s 18BH.
5 Ibid s 27(1)(ea).
6 Ibid s 27(1)(ac).
7 Ibid s 27(1)(ae). See also s 18BI.
8 Ibid s 18BB(2)(a).
9 Ibid ss 18BB(2)(b)–(c), (6)–(7).
10 Ibid s 18BB(3)(a).
11 *Legislative Instruments Act 2003* (Cth) s 44(2), item 44; *Legislative Instruments Regulations 2004* (Cth) sch 2 cl 8. Note that an approval of a variation of a privacy code, a revocation of an approval of a privacy code, or a revocation of a variation of a privacy code are also legislative instruments that are not subject to disallowance: *Legislative Instruments Act 2003* (Cth) sch 2 cls 8A, 8B.

Register of Approved Privacy Codes on the website of the Office of the Privacy Commissioner (OPC) and two code applications are being considered by the OPC.[12]

Code development process

48.6 Before the Commissioner can approve a code, he or she must be satisfied that members of the public have been given an adequate opportunity to comment on a draft of the code.[13] This requirement for public consultation is just one part of the process involved in developing a code. The *Guidelines on Privacy Code Development* (Code Guidelines) issued by the OPC in 2001 set out the detailed process involved in making a privacy code, including requirements in relation to NPP equivalence, explanatory material, coverage, voluntary membership, code review and drafting standards. In deciding whether to approve a privacy code, the Commissioner may consider the matters specified in the Code Guidelines.[14]

48.7 Following various comments from stakeholders about the complex and costly code approval process, the OPC review of the private sector provisions of the *Privacy Act* (OPC Review) recommended that the OPC review the Code Guidelines with a view to simplifying them.[15]

48.8 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the provisions for approving privacy codes were appropriate and effective, whether privacy codes were an appropriate method of regulating and complying with the Act, and why privacy codes had been so little used.[16]

48.9 The OPC submitted that, 'given the lack of take up in codes and the revocation of the only code that established its own complaint handling process, it is reasonable to conclude that the code making provisions have not been highly successful in their current form'.[17] The OPC raised several issues with codes, one being that there is tension between the concept of national consistency and industry privacy codes, in that a proliferation of industry codes may increase the complexity and fragmentation of privacy regulation. The OPC also noted that it had not derived any significant efficiency benefits from codes, as the Commissioner remains the complaint-handling

---

12 Codes in operation as at April 2008 were the Market and Social Research Privacy Code, administered by the Association of Market Research Organisations; the Queensland Club Industry Privacy Code, administered by Clubs Queensland; and the Biometrics Institute Privacy Code, administered by the Biometrics Institute. There was a fourth code approved by the Privacy Commissioner (the General Insurance Information Privacy Code), which was revoked on 30 April 2006. Code applications being considered by the OPC as at April 2008 were the Australian Casino Association Privacy Code and the Internet Industry Privacy Code. See Office of the Privacy Commissioner, *Privacy Codes* <www.privacy.gov.au/business> at 23 April 2008.

13 *Privacy Act 1988* (Cth) s 18BB(2)(f).

14 Ibid s 18BB(4).

15 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 47. See also discussion about codes at 166–171.

16 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–20.

17 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

body. This, in turn, raises the risk that the OPC's compliance role will become increasingly complex and cumbersome, as complaint staff will have to apply different sets of principles to different complaints.[18]

Submissions and consultations

48.10 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC identified support in submissions and consultations for the scope for co-regulation provided by Part IIIAA of the Privacy Act.[19] Particular issues with the current code provisions were identified by stakeholders, however, including that the current provisions for voluntary codes added to the complexity of the privacy regime;[20] and that the code-making process was resource intensive, with little identifiable benefit.[21]

48.11 The OPC submitted that the code provisions needed to be amended to take into account interests of efficiency and national consistency, suggesting that codes should operate in addition to the privacy principles, rather than replacing them.[22] The privacy principles would then apply as a base standard across the community (supporting national consistency) and codes would provide specific and binding guidance on how the principles should be applied in particular sectors. Other stakeholders also supported the idea that codes could prove useful in interpreting the application of privacy principles in the context of specific sectors or technologies.[23]

48.12 In DP 72, the ALRC proposed that the *Privacy Act* should be amended to specify that privacy codes approved under Part IIIAA operate in addition to the proposed UPPs and do not replace those principles. The ALRC also proposed that the Act should be amended to state that a privacy code may provide guidance or standards on how any one or more of the proposed UPPs should be applied, or are to be complied with, by the organisations bound by the code, provided such guidance or standards contain obligations that are at least equivalent to those under the Act.[24]

---

18 Ibid.

19 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

20 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

21 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

22 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

23 See, eg, Australian Direct Marketing Association, *Submission PR 298*, 29 June 2007.

24 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–9.

48.13 The majority of stakeholders who commented on this proposal supported it.[25] The Association of Market and Social Researcher Organisations and the Australian Market and Social Research Society agreed that:

> the role of Codes is to provide various industry sectors with greater clarity in respect of the particular nuances and information handling practices of the industry, enabling organisations to operate with certainty and reduce the risk of a legal challenge and material threat to the business. In contrast, application of the NPPs may not always be obvious. This has certainly been the experience in the market and social research industry. Moreover, as mentioned above, such industry codes allow a given industry voluntarily to raise the bar, affording greater protection to the public.[26]

48.14 The Public Interest Advocacy Centre (PIAC) agreed that the privacy principles should operate as the base standard, with codes simply filling in detail where necessary. In PIAC's view, this will ensure that the privacy principles are not undermined, and will 'reduce fragmentation, complexity and confusion in privacy regulation'.[27] The Department of Human Services submitted that enabling privacy codes to operate in conjunction with, rather than instead of, the UPPs, will lead to a consistent understanding and implementation of the *Privacy Act* requirements—particularly by small businesses who have limited resources available for compliance issues. The Department argued that the proposed reform also will assist health and social services providers in better understanding, and complying with, relevant privacy requirements.[28]

48.15 The Cyberspace Law and Policy Centre stressed that consultation with all stakeholders is important if the code process is going to deliver benefits. While Part IIIAA contains requirements for consultation, in the Centre's experience, the consultation process in developing codes to date has been inadequate.[29]

48.16 GE Money Australia expressed concern that the ALRC's proposal further complicated the layers of regulation that may apply to an organisation.

> It would, under the proposal, be possible for an organisation to be bound by the UPPs in addition to a Privacy Code, Regulations made under the Act that may provide more or less onerous obligations than under either the Act or the Code, Binding Rules

---

25 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; Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 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; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

26 Association of Market and Social Research Organisations and Australian Market and Social Research Society, *Submission PR 502*, 20 December 2007.

27 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

28 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

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

> issued by the Privacy Commissioner as well as needing to refer to the very extensive guidance that is to be issued by the Office of the Privacy Commissioner. It is suggested that this has the potential to be a very complex matrix of potentially overlapping obligations.[30]

ALRC's view

48.17 One of the consistent themes discussed by stakeholders in this Inquiry is the need to promote national consistency and to reduce fragmentation, complexity and confusion in privacy regulation. In support of this goal, codes should operate in addition to the privacy principles, rather than replacing them. At all times the privacy principles should operate as the base standard for agencies and organisations subject to the *Privacy Act*. Consistent with the ALRC's recommended regulatory model, set out in Chapter 4, the privacy principles only should be able to be displaced through subordinate legislation and public interest determinations. As outlined above, the ALRC has received substantial support for this view in submissions to this Inquiry.

48.18 Codes could facilitate an understanding of, or compliance with, the UPPs by an organisation bound by the code. This would resemble the operation of codes in New Zealand.[31]

48.19 Under this model, the guidelines contained in a code must impose obligations equivalent to those imposed by the relevant privacy principle. This relationship between the principles and the guidelines in a code can be illustrated as follows. A real estate industry code could prescribe an exhaustive list of information that can be considered 'necessary', under the 'Collection' principle, to collect in a tenancy application process.[32] By specifying particular types of information as those necessary to collect in a tenancy application form, the guidelines would contain equivalent obligations to the principle, as both require that only information that is necessary be collected. The code, however, would provide more detailed guidance than the principle and would assist real estate agencies to meet the policy outcome set by the principle.

Recommendation 48–1 Part IIIAA of the *Privacy Act* should be amended to specify that a privacy code:

(a) approved under Part IIIAA operates in addition to the model Unified Privacy Principles (UPPs) and does not replace those principles; and

30 GE Money Australia, *Submission PR 537*, 21 December 2007.
31 See *Privacy Act 1993* (NZ) s 46(2)(b).
32 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

(b) may provide guidance or standards on how any one or more of the model UPPs should be applied, or are to be complied with, by the organisations bound by the code, as long as such guidance or standards contain obligations that, overall, are at least the equivalent of all the obligations set out in those principles.

Binding codes

48.20 The Commissioner cannot initiate a privacy code and cannot make a code binding on organisations that do not consent to be bound. The issue of binding codes was discussed in detail in the OPC Review. Stakeholders submitted that the Commissioner should have the power to formulate and impose binding codes even where an organisation does not consent to being subject to a code. It was argued that this would be one way of solving systemic issues in privacy compliance.[33] Although support for this proposition was not universal, the OPC recommended that the Australian Government consider amending the *Privacy Act* to give the Commissioner the power to make binding codes and suggested a number of models for the power.[34] These models are discussed below.

48.21 The Senate Legal and Constitutional Reference Inquiry into the *Privacy Act* also considered binding codes, and noted the explanation given by the Commissioner on the difference between privacy codes approved under Part IIIAA and the OPC Review's proposal for binding codes:

> The idea of the binding codes that [the OPC has] suggested is to come up in other areas where perhaps they were not going to be voluntary. The NPP codes are developed on a voluntary basis. The ones that were binding could possibly be done for technology, or for an industry that was not working as well—perhaps the tenancy database area.[35]

48.22 The New Zealand Privacy Commissioner has the power to issue binding codes of practice that become part of the law.[36] The codes may modify the application of one or more of the information privacy principles by prescribing: standards that are more or less stringent than the standards prescribed by the principle; or how any one or more of the principles are to be applied, or are to be complied with.[37] The codes also may

---

33 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 145.

34 Ibid, recs 7, 44. See related recommendations in recs 16, 73. For a discussion about models, see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 46–47.

35 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 97–98.

36 *Privacy Act 1993* (NZ) pt 6. Note the Privacy Commissioner in NSW has similar powers to initiate binding privacy codes: *Privacy and Personal Information Protection Act 1998* (NSW) pt 3 div 1.

37 *Privacy Act 1993* (NZ) s 46(2).

modify the operation of the *Privacy Act 1993* (NZ) for specific industries, agencies, activities or types of personal information.[38] The Privacy Commissioner may issue a code of practice on his or her initiative. In addition, a body representing the interests of a particular class of agency, industry or profession may apply to the Privacy Commissioner for a code of practice to be issued.[39]

Prescribed industry codes under the *Trade Practices Act*

48.23 One of the models put forward by the OPC for a binding code power was Part IVB of the *Trade Practices Act 1974* (Cth) (TPA). Under the TPA, the Minister has the power to prescribe an industry code of conduct in the regulations.[40] The regulations declare the industry code to be a mandatory industry code or a voluntary industry code. A prescribed mandatory code of conduct is binding on all industry participants.[41] The Act makes the codes enforceable by prohibiting a corporation, in trade or commerce, from contravening an applicable industry code.[42]

48.24 At a practical level, formal proposals for TPA codes are initiated at the ministerial level, 'following representations from industry participants, consumers or government authorities about problems in a particular industry'.[43] As the regulator under the TPA, the Australian Competition and Consumer Commission is responsible for promoting compliance with codes by providing education and information and, where necessary, by taking enforcement action. Since the introduction of these provisions in 1998, three mandatory codes of conduct have been prescribed under the TPA.[44]

Industry codes and standards in the *Telecommunications Act*

48.25 Another model put forward by the OPC was Part 6 of the *Telecommunications Act 1997* (Cth). Under this Act, bodies and associations that represent sections of certain industries may develop industry codes, which may be registered by the Australian Communications and Media Authority (ACMA). Compliance with the code is voluntary unless otherwise directed by ACMA.[45] In addition, ACMA can request a body or association to develop an industry code.[46] If the request is refused or the code

38 Ibid s 46(3).
39 Ibid s 47.
40 *Trade Practices Act 1974* (Cth) pt IVB.
41 Ibid s 51AE.
42 Ibid s 51AD.
43 J Hockey, *Prescribed Codes of Conduct: Policy Guidelines on Making Industry Codes of Conduct Enforceable under the Trade Practices Act 1974* (1999) Australian Government Treasury, 6.
44 See *Trade Practices (Industry Codes – Franchising) Regulations 1998* (Cth); *Trade Practices (Industry Codes – Oilcode) Regulations 2006* (Cth); *Trade Practices (Horticultural Code of Conduct) Regulations 2006* (Cth).
45 *Telecommunications Act 1997* (Cth) s 121.
46 Ibid s 118.

prepared following a request is not registered by ACMA, or if an existing code is deficient, ACMA may determine an 'industry standard'.[47]

48.26 In making an industry standard, ACMA must be satisfied that it is necessary or convenient for it to determine a standard in order to: provide appropriate community safeguards in relation to the matter; or otherwise regulate adequately participants in that section of the industry.[48] Compliance with an industry standard is mandatory; each participant in the section of an industry to which the standard applies must comply with the standard.[49] Breach of a standard is subject to a civil penalty and ACMA may issue a formal warning if a person contravenes an industry standard registered under Part 6.[50] An industry standard is a disallowable instrument and the Act specifies that ACMA must consult with members of the public, consumer bodies and relevant regulators before determining or varying an industry standard.[51]

Submissions and consultations

48.27 In IP 31, the ALRC asked whether the Commissioner should have the power, on his or her initiative, to develop and impose a binding code on agencies or organisations.[52] In response, a few stakeholders argued that the Commissioner should have such a power.[53] Stakeholders, including the OPC, suggested that such a power would be a useful means of addressing systemic privacy issues. This view was not unanimous, however, and other stakeholders did not think a binding code-making power would be appropriate in a light-touch regime such as the *Privacy Act*.[54]

48.28 In DP 72, the ALRC proposed that the Commissioner be empowered to request the development of a privacy code to be approved by the Commissioner pursuant to s 18BB of the *Privacy Act*; and to develop and impose a privacy code that applies to designated agencies and organisations.[55]

48.29 In response to DP 72, there continued to be strong support among stakeholders for a binding code-making power.[56] Anglicare Tasmania submitted that under the current system—given that the development of a code can only be initiated by the industry concerned—it seems highly unlikely for an industry that was not complying

---

47 Ibid ss 123, 125.
48 Ibid s 123(1)(c).
49 Ibid s 128.
50 Ibid s 129.
51 Ibid s 132–135A.
52 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–20.
53 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Privacy NSW, *Submission PR 193*, 15 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.
54 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
55 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 44–10.
56 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Veda Advantage, *Submission PR 498*, 20 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; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

with the *Privacy Act* to take the step of initiating the development of a code. For this reason, Anglicare Tasmania supported giving the Commissioner the power to issue binding codes when there are systemic problems within a particular industry and the industry itself is reluctant to address them.[57]

48.30 PIAC submitted that the ability to develop binding codes would enable the Privacy Commissioner to take a more proactive role in privacy regulation where there is a need for detailed regulation of specific sectors or for specific technologies. It noted, however, that it would be essential to ensure that the Privacy Commissioner is funded adequately for this task.[58]

48.31 A number of stakeholders cautioned against creating another level of regulation in industries where there was already a high compliance burden. The Australasian Compliance Institute, for example, stated:

> The financial services industry has adopted various legally or contractually enforceable codes, such as the EFT Code of Conduct, the Code of Banking Practice, Financial Planners Code of Ethics and Rules of Professional Conduct, General Insurance Code of Conduct and IFSA Membership Standards. Existing codes embrace privacy considerations and privacy issues in the context of the industry or conduct it is seeking to regulate. Introducing additional industry codes would create multi layered regulation, increasing the compliance burden on industry. It could impose additional cost and resources in training staff on the various codes and could lead to staff and customer confusion.[59]

48.32 It was also argued that the imposition of industry, organisation or agency specific codes would complicate privacy laws and impose unduly onerous obligations on some organisations. In the view of some stakeholders, the UPPs alone should set out the information-handling standards to which agencies and organisations should adhere.[60]

ALRC's view

48.33 As discussed in Chapter 4 and above, the ALRC's approach to reform of the *Privacy Act* retains the ability of organisations and industries to flesh out the requirements of the privacy principles in voluntary privacy codes approved by the Privacy Commissioner under Part IIIAA.

48.34 As has been noted throughout this Report, a key goal of the ALRC's recommendations is to reduce the complexity of Australia's privacy regulation.

---

57 Anglicare Tasmania, *Submission PR 514*, 21 December 2007. This view was shared by the Australian Lawyers Alliance: Australian Lawyers Alliance, *Submission PR 528*, 21 December 2007.

58 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

59 Australasian Compliance Institute, *Submission PR 419*, 7 December 2007. See also Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

60 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007.

Although many submissions supported the inclusion of a binding code-making power, the ALRC shares the concerns raised by other stakeholders that empowering the Commissioner to initiate a binding code could result in multiple levels of regulation, and lead to confusion and fragmentation of the federal privacy regime. The ALRC therefore does not recommend that a binding code-making power be included in the Act.

48.35 The ALRC's recommended regulatory model does, however, accommodate industry-developed regulations that would allow for a particular sector or technology to derogate from the UPPs. These would not be approved under Part IIIAA, as privacy codes under the current and recommended Part IIIAA code provisions cannot derogate from the principles. Instead, these codes would be prescribed following the model in the TPA. Under this model, the relevant minister can prescribe an industry code of conduct which is passed by Parliament in the regulations, using the ALRC's recommendation for a regulation-making power. The regulations could declare the industry code to be a mandatory industry code, and binding on all industry participants.[61]

61 This model of adopting regulations which derogate from the UPPs is recommended by the ALRC in relation to credit reporting information and health information. See Chs 54, 60.

49. Investigation and Resolution of Privacy Complaints

Contents

Introduction

49.1 The *Privacy Act 1988* (Cth) provides an avenue for individuals to complain about acts or practices of an agency or organisation that may be an interference with their privacy. The Act vests power in the Privacy Commissioner (Commissioner) to investigate, conciliate and make determinations to finalise complaints.

49.2 This chapter considers the investigation and resolution of complaints under the *Privacy Act*. It examines concerns about accountability and transparency in the Act and in the policies and procedures of the Office of the Privacy Commissioner (OPC) with regard to complaint handling. The chapter also considers some particular issues raised by stakeholders relating to representative complaints, preliminary inquiries, and the conduct of investigations.

Investigating privacy complaints

Background

49.3 The Commissioner's powers to investigate complaints of a breach of the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) are established in separate paragraphs of s 27(1) of the *Privacy Act*.[1] These powers are activated by a 'complaint'. The Act confers rights on individuals to complain to the Commissioner about acts or practices that may be an interference with individuals' privacy rights, as created by the Act.[2]

Matters the Commissioner must not investigate

49.4 The Commissioner generally is required to investigate an act or practice if it may be an interference with an individual's privacy and a complaint has been made about it under s 36.[3] The Commissioner must not investigate a complaint, however, if the complainant did not first complain to the respondent, unless the Commissioner considers that it was not appropriate for the complainant to do so.[4] The Commissioner also must cease investigating if certain offences have been committed, or where the Auditor-General already is investigating the matter.[5] These last two situations are discussed later in this chapter.

Discretion not to investigate or to defer investigation

49.5 The Commissioner has the discretion to decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under s 36, or accepted under s 40(1B), where the:

- act or practice is not an interference with privacy; the complaint was made over 12 months after the complainant became aware of the act or practice; the

---

1 *Privacy Act 1988* (Cth) ss 27(1)(a), 27(1)(ab).

2 Ibid s 36. Note, there is no right to complain to the Commissioner about acts or practices of an organisation bound by an approved privacy code where the code contains a procedure for making and dealing with complaints to an adjudicator, and the code is relevant to the act or practice in question: see s 36(1A).

3 Ibid s 40(1). The power to investigate on the Commissioner's own motion is discussed in Ch 50.

4 Ibid s 40(1A). In practice, the OPC requires that complainants provide it with a copy of their letter to the respondent and a copy of any response received by the complainant. The OPC requires that the complainant give the respondent 30 days to reply to the letter of complaint: see Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007.

5 *Privacy Act 1988* (Cth) ss 49, 51.

complaint is frivolous, vexatious, misconceived or lacking in substance; the act or practice is the subject of an application under another federal, state or territory law and the complaint is being dealt with adequately under that law; or another law provides a more appropriate remedy for the complaint;[6]

- complainant has complained to the respondent about the act or practice and the respondent is dealing adequately with the complaint or has not yet had an adequate opportunity to deal with the complaint;[7] or

- respondent has applied for a public interest determination and the Commissioner is satisfied that the interests of persons affected by the act or practice would not be prejudiced unreasonably if the investigation were deferred until the application has been disposed of.[8]

Submissions and consultations

49.6 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC noted a number of concerns raised by stakeholders about the requirement to complain to the respondent before complaining to the Privacy Commissioner, and the limitations on the Commissioner's ability to dismiss minor or stale complaints.

49.7 The ALRC made a number of proposals to expand the Commissioner's powers under s 41, including that the Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made, if the Commissioner is satisfied that:

- the complainant has withdrawn the complaint;

- the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint; or

- an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.[9]

---

6 See Ibid s 41(1).
7 Ibid s 41(2).
8 Ibid s 41(3).
9 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–1.

49.8 This proposal was supported by a number of stakeholders.[10] Some stakeholders, however, expressed concern about giving the Commissioner a broader power to decline to investigate. These concerns were based on a perception that the OPC did not have a strong record in investigating complaints, and would be likely to refuse complaints even where there were potentially serious and systemic concerns.[11] The Public Interest Advocacy Centre (PIAC) agreed with the ALRC that there was a need for systemic issues to be addressed in privacy legislation. It argued, however, that:

> this should not be at the expense of individual complaints. In PIAC's experience, many systemic issues only become evident as a result of a number of individual complaints about the same or similar issues.[12]

49.9 The Cyberspace Law and Policy Centre broadly supported the proposal, but was concerned that allowing the Commissioner to decline to investigate where it is not warranted in the circumstances would be open to abuse. In the Centre's view, where the Commissioner makes such an assessment, a complainant should be given the right to require a determination under s 52 of the *Privacy Act*.[13]

ALRC's view

49.10 A central tension in the regulation of compliance with the *Privacy Act* is how to strike a balance between resolving individual complaints and remedying systemic issues. By systemic issues, the ALRC is referring to 'issues that are about an organisation's or industry's practice rather than about an isolated incident'.[14] Systemic issues can be distinguished from issues that have no implications beyond the immediate actions and rights of the parties to the complaint.[15] They can be identified out of the consideration of a single complaint, however, 'because the effect of the particular issue will clearly extend beyond the parties to the complaint'.[16]

---

10 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 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; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

11 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Consumer Action Law Centre, *Submission PR 510*, 21 December 2007.

12 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

14 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 130 fn 102.

15 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999, [PS 139.131]–[PS 139.133].

16 Ibid, [PS 139.131]–[PS 139.133]. A similar definition was put forward in Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

49.11 A compromise needs to be made between addressing individual complaints and addressing systemic issues. The compromise recommended by the ALRC is to give the Commissioner more discretion not to investigate individual complaints in certain circumstances. First, the Commissioner should be given a discretion not to investigate an act or practice if he or she is satisfied that an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances. This discretion would enable the Commissioner to dismiss trivial complaints, or complaints that have no prospect of a practical or satisfactory resolution. The same discretion is available to the Commonwealth Ombudsman[17] and a similar test is used in state legislation such as the *Anti-Discrimination Act 1977* (NSW).[18] While the ALRC notes the concerns of stakeholders based on past experience, the OPC has worked steadily over the past two years, with additional funding, to improve the overall efficiency of its complaint-handling processes. This should allow the OPC to allocate more resources to important investigations.[19]

49.12 The Commissioner's powers to dismiss stale complaints also should be clarified. The *Privacy Act* should be amended to give the Commissioner the specific discretion to cease investigating a complaint that has been withdrawn by the complainant; or where the Commissioner has had no substantive response from the complainant for a certain period, following a request by the Commissioner for a response in relation to the complaint.[20]

49.13 The ALRC does not recommend any reform to the requirement of first complaining to the respondent. The ALRC agrees with the OPC that where a complaint can be resolved between the complainant and respondent without involving the OPC, this is likely to be the most efficient means of resolving it. This approach also is consistent with other privacy legislation and the approach taken in external dispute resolution (EDR) schemes such as the Banking and Financial Service Ombudsman (BFSO) and the Telecommunications Industry Ombudsman (TIO).[21] The obligation of complaining first to the respondent, however, should be supported by agencies and organisations adopting internal dispute resolution processes and making the avenues of complaint clear in their Privacy Policies.[22]

---

17 *Ombudsman Act 1976* (Cth) s 6.

18 *Anti-Discrimination Act 1977* (NSW) s 92(1)(a)(iii).

19 In 2006–07, the OPC closed 1,210 complaints, 7% more than the 1,131 complaints closed in 2005–06: Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [3.3.2].

20 Examples of similar provisions include: *Health Records Act 2001* (Vic) s 53(1); *Information Privacy Act 2000* (Vic) s 30.

21 See, eg, *Information Privacy Act 2000* (Vic) s 29; *Health Records Act 2001* (Vic) s 51; *Ombudsman Act 1976* (Cth) s 6; Banking and Financial Services Ombudsman, *About Us* <www.abio.org.au> at 5 May 2008; *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [5].

22 This is consistent with Rec 24–1.

Recommendation 49–1 The *Privacy Act* should be amended to provide that, in addition to existing powers not to investigate, the Privacy Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made, or which the Commissioner has accepted under s 40(1B), if the Commissioner is satisfied that:

(a) the complainant has withdrawn the complaint;

(b) the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint; or

(c) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.

Transferring complaints to other bodies

Background

49.14 The *Privacy Act* contemplates the use of other bodies to resolve privacy complaints. For example, a privacy code approved under the Act may provide procedures for dealing with complaints under the code. The *Privacy Act* also vests the Commissioner with discretion to refer complaints to other bodies. Where the Commissioner forms the view that the complaint could have been made to the Human Rights and Equal Opportunity Commission (HREOC), the Commonwealth Ombudsman, the Postal Industry Ombudsman or the Public Service Commissioner, and would be dealt with more effectively or conveniently by one of those bodies, the Commissioner may decide not to investigate, or further investigate, the matter, and can transfer the complaint to the relevant body.[23]

49.15 Independent of the *Privacy Act* provisions, there are also several EDR schemes that have jurisdiction to deal with privacy complaints under their terms of reference, including the BFSO and the TIO.[24] Many credit providers already are members of industry-based EDR schemes, notably those involving the BFSO and the TIO. Veda Advantage, the main consumer credit reporting agency, also is a member of the BFSO. Issues regarding credit providers and EDR schemes are discussed in more detail in Chapter 59.

---

23 *Privacy Act 1988* (Cth) s 50.

24 See Banking and Financial Services Ombudsman, *Terms of Reference*, 1 December 2004, [3.1]; *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [4.1].

49.16 In its 2005 review of the private sector provisions of the *Privacy Act* (OPC Review), the OPC considered improving liaison with overlapping complaint handlers, to maximise efficiency and minimise confusion and costs for individuals and organisations.[25] In 2006, the OPC entered into a memorandum of understanding with the Commonwealth Ombudsman, to 'facilitate the exchange of information, subject to the expectations of the individuals concerned, so that individuals with complaints can continue to have their concerns dealt with effectively and efficiently'.[26]

Submissions and consultations

Referrals to EDR Schemes

49.17 In DP 72, the ALRC identified support in submissions and consultations for empowering the Commissioner to transfer complaints to other bodies, and in particular, EDR schemes. The ALRC proposed that the *Privacy Act* should be amended to empower the Commissioner to decline to investigate, or investigate further, a complaint that already is being handled by an approved EDR scheme. The Commissioner also should be empowered both to decline to investigate a complaint and refer it on to an EDR scheme, where the Commissioner is satisfied that the complaint would be handled more suitably by that scheme.[27]

49.18 The proposal was supported by a number of stakeholders, including the OPC.[28] Privacy advocates supported the proposal on the basis that:

- the EDR scheme is approved by the OPC;[29] and
- there are appropriate review and appeal mechanisms in place.[30]

---

25 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159–160.

26 Office of the Privacy Commissioner, 'Ombudsman and Privacy Commissioner to Streamline Joint Complaint Handling Processes' (Press Release, 30 November 2006).

27 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–2.

28 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Federal Police, *Submission PR 545*, 24 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

29 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

30 Ibid; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

49.19 PIAC also submitted that the OPC should publish a list of approved EDR schemes on its website and that the criteria for approval should include a mechanism for reporting to the OPC on serious or systemic conduct.[31]

49.20 Two stakeholders did not support the proposal. In the view of these stakeholders, the OPC should be the only body to resolve privacy complaints as this would ensure consistency in approach.[32]

Referrals to state bodies

49.21 The ALRC also proposed that the Commissioner's current delegation power in the *Privacy Act* be extended to empower the Commissioner to delegate to a state or territory authority all or any of the powers, including a power conferred by s 52, in relation to complaint handling conferred on the Commissioner by the *Privacy Act*.[33]

49.22 The OPC did not support this proposal, on the basis that it would introduce a level of complexity and uncertainty into the complaint-handling process. In the OPC's view, if a function were delegated 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 the argument of 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.[34]

49.23 The OPC also argued that there would be resource implications arising from the proposal.

> The Office is aware of other regulatory environments where such models have been adopted, resulting in significant complexity, uncertainty and funding difficulties. Such a model would require the Privacy Commissioner to be confident that the other complaint handling agency would interpret and apply the principles consistently, as well as follow the same processes as the Office. This could require significant training and development in the Office and would have resource implications. It would also be necessary to ensure that, where a determination was made, any decisions regarding remedies would be equivalent to the decision that would be made by the Privacy Commissioner.[35]

---

31 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

32 Confidential, *Submission PR 536,* 21 December 2007; Confidential, *Submission PR 519,* 21 December 2007.

33 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–3.

34 Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007. Others that did not support the proposal included: Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Confidential, *Submission PR 519,* 21 December 2007.

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

49.24 The Australian Privacy Foundation stated that it only would support the ALRC's proposal if the proposal 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*.[36]

49.25 The Cyberspace Law and Policy Centre agreed that if the Commissioner transferred a complaint, this should be done only on the basis that the state or territory body is required to report to the Commissioner the details and outcome of the complaint resolution, and the Commissioner is required to publish those details to the same extent as any other complaint investigated by the Commissioner.[37]

49.26 A number of other stakeholders, however, expressed support for the ALRC's proposal.[38] For example, Medicare Australia expressed the view that delegation could be helpful where the other authority can address issues other than the handling of personal information that might form part of the complaint, or where local knowledge could assist with resolution.[39]

49.27 In DP 72, the ALRC also proposed that the Commissioner should consider delegating the power to handle health information complaints under the *Privacy Act* to state and territory health complaint agencies.[40] Submissions and consultations dealing with this specific issue are discussed in Chapter 60. It is noted that the ALRC received support for that proposal from a diverse range of stakeholders.

ALRC's view

Transferring complaints to EDR schemes

49.28 There is merit in recognising more formally the role of EDR schemes in handling privacy complaints. Schemes such as the BFSO and the TIO already resolve privacy complaints under their terms of reference and provide an efficient and binding avenue of complaint resolution for complainants and respondents.[41]

---

36 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. This view was shared by PIAC: Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

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

38 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 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; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

39 Medicare Australia, *Submission PR 534*, 21 December 2007.

40 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 56–1.

41 Under the Terms of Reference of the BFSO, a determination issued by the BFSO is binding on the complainant and respondent if the complainant agrees to accept it in full and final settlement of the subject matter of the dispute: Banking and Financial Services Ombudsman, *Terms of Reference*, 1 December 2004, [7.12]. A similar approach is taken by the TIO: *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [6.1].

49.29 The *Privacy Act* should be amended to empower the Commissioner to decline to investigate, or investigate further, a complaint that already is being handled by a recognised EDR scheme. The Commissioner also should be empowered to decline to investigate a complaint and refer it on to an EDR scheme, where the Commissioner is satisfied that the complaint would be handled more suitably by the scheme. A greater role for EDR schemes in dealing with privacy complaints has the potential to increase efficiency in dispute resolution and to provide parties with a one stop shop for complaints that are partly about privacy and partly about service delivery.

49.30 In Chapter 59, the ALRC discusses an OPC concern that it be required to 'approve' an EDR scheme for the purposes of declining a complaint or referring its power. The use by the ALRC of the term 'approved' in the original proposal was not intended to indicate that the OPC would need to establish its 'own separate benchmarks and an overall EDR scheme approval process'.[42] This would be a considerable burden on the OPC, and may duplicate the processes of other agencies that approve schemes as part of the legislation they administer. To make this distinction clearer, the recommendation should refer to OPC 'recognition', rather than approval, of EDR schemes.[43]

49.31 The ALRC notes that the Australian Securities and Investments Commission (ASIC) standard for approved EDR schemes requires that schemes report to ASIC on systemic issues and serious misconduct.[44] A similar reporting mechanism would be valuable in the privacy context to increase the OPC's awareness of systemic issues.

49.32 Following implementation of these reforms, the OPC should publish a list of recognised EDR schemes on its website, to increase transparency and awareness of the referral process.

Referring complaints to state bodies

49.33 There could be similar benefits in using existing state complaint-handling bodies for the investigation and resolution of complaints under the *Privacy Act*. This would facilitate complaints being handled by local bodies, which can be more efficient and convenient for the complaint handler and the parties to the complaint.

49.34 The most effective and flexible mechanism to facilitate this movement of complaints is to extend the Commissioner's delegation function in s 99 of the *Privacy Act*. As noted in DP 72, the Commissioner would not be required to delegate his or her functions unless he or she was of the view that it would be appropriate or effective to do so.

---

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

43 For example, in the context of credit reporting complaints, the OPC can be expected to recognise EDR schemes already approved by ASIC under the *Corporations Act 2001* (Cth) and those with another statutory basis, such as the TIO. The OPC could also recognise schemes that are certified by an independent third party as complying with the ASIC standard and other similar instruments: see Ch 59.

44 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999, [PS 139.59].

49.35 It is important to note that under such an arrangement, the state or territory authority would be empowered both to handle complaints under the *Privacy Act* and to exercise the powers of the Privacy Commissioner. The handling of complaints would, therefore, be consistent with the OPC's complaint-handling process. The Commissioner also could include other stipulations in the arrangements surrounding any such delegation. The Commissioner should consider issues of capacity, expertise, and resources before entering into such an arrangement with a state or territory authority.

49.36 While the ALRC notes concerns about consistency in decision making, this concern could arise in any context where there are multiple decision makers. As long as the principles and powers under which the decision maker operates are the same, significant issues of inconsistency should not arise.

49.37 This recommendation is consistent with the view expressed in Chapter 60, that the Commissioner should consider delegating, where appropriate, the power to handle complaints under the *Privacy Act* in relation to health information to state and territory health complaint agencies.

Guidance

49.38 Given the ALRC's recommendations to empower the Commissioner to transfer complaints to EDR schemes and delegate complaint-handling powers to state bodies, it would be beneficial to provide guidance on these different avenues of complaint handling to agencies, organisations and potential complainants. This could be part of a document setting out the OPC's complaint-handling policies and procedures.[45]

Recommendation 49–2 The *Privacy Act* should be amended to empower the Privacy Commissioner to decline to investigate a complaint where:

(a) the complaint is being handled by an external dispute resolution scheme recognised by the Privacy Commissioner; or

(b) the Privacy Commissioner considers that the complaint would be more suitably handled by an external dispute resolution scheme recognised by the Privacy Commissioner, and should be referred to that scheme.

45 See Rec 49–8.

Recommendation 49–3 The *Privacy Act* should be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers in relation to complaint handling conferred on the Commissioner by the Act.

Resolution of privacy complaints

Model under the *Privacy Act*

49.39 The *Privacy Act* provides two formal ways of resolving a complaint following an investigation. First, the Commissioner can endeavour, by conciliation, to effect a settlement between the complainant and respondent.[46] Secondly, the Commissioner can make a determination either dismissing the complaint or finding the complaint substantiated.[47]

Conciliation

49.40 The Commissioner is given the general direction in complaints against both agencies and organisations, to attempt, by conciliation, to effect a settlement of the matters that gave rise to the investigation. The Commissioner is required to conciliate a complaint only where he or she considers it appropriate to do so.[48] In contrast to other privacy legislation, the *Privacy Act* does not set out detailed provisions on how to conduct the conciliation process.[49]

49.41 In practice, the OPC will conciliate complaints where it thinks there is enough evidence to support the complaint. The OPC conciliates by writing or telephoning the respondent to see if it agrees to the complainant's solution, or bringing the parties together in a conciliation conference.[50] If the parties reach an agreement during conciliation, the OPC closes the file on the basis that the respondent has dealt adequately with the matter. The OPC received a total of 1,094 complaints in 2006–07,[51] and closed 1,210 complaints, representing a 7% increase on the number closed in 2005–06.[52] Of the complaints closed following an investigation, the typical outcomes

---

46 *Privacy Act 1988* (Cth) ss 27(1)(a), 27(1)(ab).

47 Ibid s 52.

48 Ibid ss 27(1)(a), 27(1)(ab).

49 See, eg, the conciliation provisions in *Information Privacy Act 2000* (Vic) pt 5 div 3; *Health Records Act 2001* (Vic) pt 6 div 3; *Information Act 2002* (NT) ss 110–113 (in relation to mediation). See also the proposed provisions in Information Privacy Bill 2007 (WA) pt 5 div 2.

50 See Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007.

51 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [3.3.1].

52 Ibid, [3.3.2].

involved apologies to complainants, changes to database systems, correction of records, provision of access to records and compensation.[53]

49.42 If the parties cannot reach agreement during conciliation, the Commissioner will make a decision about how the complaint should be resolved. That decision may be that the respondent has made the complainant a reasonable offer which has not been accepted, in which case the Commissioner may close the file on the grounds that the respondent has dealt with the matter adequately, even if the complainant does not agree. Alternatively, the Commissioner may decide that the respondent has not made a reasonable offer, in which case the Commissioner can make a determination instructing the respondent on how to resolve the complaint, including ordering the respondent to apologise, pay compensation or change its practices.[54]

Determinations

49.43 As noted above, the Commissioner can make a determination dismissing the complaint, or can find a complaint substantiated and make a determination that includes one or more of the following declarations that:

- the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct;[55]
- the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;[56]
- the complainant is entitled to a specified amount by way of compensation for any loss or damage;[57] or
- it would be inappropriate for any further action to be taken in the matter.[58]

---

53 Ibid, [3.3.2]. See also Table 3.5.

54 This is summarised from Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007.

55 *Privacy Act 1988* (Cth) s 52(1)(b)(i).

56 Ibid s 52(1)(b)(ii). 'Loss or damage' is defined in s 52(1A).

57 Ibid s 52(1)(b)(iii). The *Privacy Act* does not limit the monetary compensation that the Commissioner may award to a complainant: Australian Institute of Company Directors, Office of the Federal Privacy Commissioner and Information and Privacy Commissioner Ontario, *Privacy and Boards: What You Don't Know Can Hurt You* (2004), 11; *Rummery and Federal Privacy Commissioner* [2004] AATA 1221, [26]–[29]. See s 52(4)–(6) in relation to compensation orders in representative complaints. The Commissioner also can make a declaration that the complainant is entitled to a specified amount as reimbursement for expenses reasonably incurred in connection with the complaint: *Privacy Act 1988* (Cth) s 52(3).

58 *Privacy Act 1988* (Cth) s 52(1)(b)(iv).

49.44 A determination of the Commissioner under s 52(1) is not binding or conclusive between any of the parties to the determination.[59] This reflects the fact that Commonwealth judicial power only can be exercised by a court in accordance with Chapter III of the *Australian Constitution*.[60] Enforcement of determinations is discussed in Chapter 50.

49.45 There have been eight complaint determinations made since the *Privacy Act* commenced in 1989, with the most recent being in 2004.[61] Following a number of submissions from stakeholders commenting on the limited exercise of the determination power and suggesting that complainants should be able to compel the Commissioner to make a determination, the OPC Review recommended that it would consider circumstances in which it might be appropriate to make greater use of the Commissioner's power to make determinations under s 52.[62] Since then, the OPC has reviewed the use of the s 52 determination powers and identified situations where it may proceed more quickly to a determination, including where the:

- interests of the parties will be better served by the opportunity to make formal submissions to the Commissioner;
- issues in the complaint are not clear and the Commissioner will need to make findings; or
- complaint is not amenable to conciliation, or conciliation has failed.[63]

49.46 The OPC also clarified that determinations would 'not necessarily be limited to the most serious cases, nor will determinations issued by the Commissioner necessarily be punitive'.[64]

49.47 The other issue with determinations identified by stakeholders in the OPC Review was the inability of the Commissioner to prescribe remedies to prevent future harm. The issue was said to be illustrated in determinations made against a residential tenancy database operator in 2004. In those determinations, the Commissioner found that, while he could declare that the respondent should not repeat or continue conduct

---

59 Ibid s 52(1B).

60 C Saunders, 'The Separation of Powers' in B Opeskin and F Wheeler (eds), *The Australian Federal Judicial System* (2000) 3, 14, 15–16, 25. See, eg, *Huddart, Parker & Co Pty Ltd v Moorehead* (1909) 8 CLR 330, 357; *Waterside Workers' Federation of Australia v JW Alexander Ltd* (1918) 25 CLR 434, 442; *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254, 281–282; *Brandy v Human Rights and Equal Opportunity Commission* (1995) 183 CLR 245.

61 Office of the Privacy Commissioner, *Complaint Case Notes, Summaries and Determinations* (2007) <www.privacy.gov.au/act/casenotes/index.html> at 15 May 2008.

62 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 37, 42. See also the discussion at 139, 144.

63 Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2, 2.

64 Ibid, 2.

that constitutes an interference with the privacy of an individual, he did not have the power to prescribe how the respondent should act in the future.[65] Following concerns from stakeholders that this restriction limited the Commissioner's ability to address systemic issues, the OPC recommended that the Government consider amending the *Privacy Act* to expand the remedies available under a determination to include giving the Commissioner power to require a respondent to take steps to prevent future harm arising from systemic issues.[66] In its response to the OPC Review, the Australian Government agreed with this recommendation.[67]

Submissions and consultations

49.48 In DP 72, the ALRC identified a number of concerns raised by stakeholders about the complaint-resolution process under *Privacy Act* and the OPC's procedures. These concerns were grouped into: issues with the framework for conciliation in the Act; the difficulty in distinguishing between the stages of investigation, conciliation and determination under the Act; and the timing of these stages. Concerns also were expressed about the limited use of the determinations power by the Commissioner, with suggestions made that complainants should have the right to compel a determination where conciliation fails. The third area of concern was the limited ability for a determination to effect systemic change, as it cannot prescribe positive steps for a respondent to take to achieve compliance with the Act.[68]

49.49 Having regard to these issues, the ALRC made several proposals to clarify the complaint-handling process under the *Privacy Act*.

Clarifying the Commissioner's functions

49.50 First, the ALRC proposed that s 27(1)(a) and (ab) should be amended to clarify that the Commissioner's functions in relation to complaint handling include:

- receiving complaints about an act or practice that may be an interference with the privacy of an individual;
- investigating the act or practice about which a complaint has been made; and

65 See Office of the Federal Privacy Commissioner, *Complaint Determination No 1 of 2004*, 1 April 2004. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 136.

66 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 44.

67 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), [Item 44].

68 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [45.38]–[45.50].

- where the Commissioner considers it appropriate to do so, and at any stage after acceptance of the complaint, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the complaint or to make a determination in respect of the complaint under s 52.[69]

49.51 Stakeholders who commented on this proposal supported it unanimously.[70]

New conciliation provisions

49.52 Secondly, the ALRC proposed that *Privacy Act* should be amended to include new provisions dealing expressly with conciliation, and that the provisions should give effect to the following:

(a) If, at any stage after receiving the complaint, the Commissioner considers it reasonably possible that the complaint may be conciliated successfully, he or she must make all reasonable attempts to conciliate the complaint.

(b) Where, in the opinion of the Commissioner, all reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination.

(c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.[71]

49.53 The OPC agreed with aspects of this proposal, but suggested the following changes:

- to be consistent with other proposals, the reference in (a) to 'receiving' a complaint should be changed to 'accepting';

- the requirement that the Commissioner make 'all reasonable attempts' to conciliate is too uncertain and should be changed to 'reasonable attempts'; and

---

69 Ibid, Proposal 45–4.

70 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 Federal Police, *Submission PR 545*, 24 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.

71 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–5.

- a complainant or respondent should not be able to require that the complaint be resolved by determination. In the OPC's view, where the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner should be required to notify the complainant and respondent that conciliation has failed. The Commissioner must then decide whether to decline the complaint, investigate or investigate further, or resolve the complaint by determination.[72]

49.54 A majority of stakeholders, however, were supportive of the proposal, and in particular, allowing that a determination be requested where conciliation had failed.[73] PIAC argued that:

> A major problem with the current regulatory system has been the failure of successive Privacy Commissioners to make determinations under section 52 and the inability of plaintiffs or defendants to compel them to do so. If the plaintiff or respondent can require that a matter be resolved by determination, the number of determinations made by the Privacy Commissioner should increase and there is at last potential for a solid body of jurisprudence to develop about the interpretation of the provisions of the Act.[74]

49.55 The Australian Policy Foundation and the Cyberspace Law and Policy Centre both submitted that an applicant also should have the right to require a determination whenever the Commissioner proposes to refuse to investigate (or investigate further) a complaint.[75]

49.56 One stakeholder took the view that giving complainants the power to ask for a determination would give them significant leverage to force respondents to agree to compensation to avoid the 'time-consuming' formal determination process.[76]

Declarations for action

49.57 Thirdly, the ALRC proposed that s 52 of the *Privacy Act* should be amended to empower the Commissioner to make a declaration in a determination that an agency or

---

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

73 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007.

74 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

75 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

76 Confidential, *Submission PR 536*, 21 December 2007.

respondent must take specified action within a specified period for the purpose of ensuring compliance with the Act.[77]

49.58 A number of stakeholders commented on this proposal, with most expressing support.[78] Telstra Corporation Limited did not support the proposal, however, on the basis that 'it is inappropriate to empower the Privacy Commissioner to determine specific compliance measures for organisations'. In Telstra's view, under an outcome-based regulatory regime, organisations are the correct bodies to determine what measures should be adopted within their own businesses to achieve compliance.[79]

ALRC's view

Framework for conciliation and determinations

49.59 The current relationship in the *Privacy Act* between conciliation and determination is not clear. An explanation of the intended relationship was provided in the Second Reading Speech for the Privacy Bill 1988 (Cth), where the then Attorney-General stated:

> Under the Bill an individual will be able to complain to the Privacy Commissioner about alleged interferences with privacy, who will attempt to resolve the allegations by conciliation and, failing that, making binding determinations against agencies, including determinations for compensation and costs.[80]

49.60 The relationship between conciliation and determination, and the Commissioner's functions in relation to each, should be clarified in the *Privacy Act*. The ALRC recommends that the *Privacy Act* be amended to clarify the Commissioner's functions in relation to complaint handling and the process to be followed when a complaint is received. This could be achieved by amending s 27(1)(a) and (ab) to clarify the Commissioner's functions relating to privacy complaints, including the functions of receiving and investigating complaints, conciliating where appropriate or making a determination. Consistent with the recommendation that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity,[81] this amendment would, if implemented, provide a succinct summary of the Commissioner's functions in relation to the investigation and resolution of privacy

---

77 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–6.

78 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; 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; P Youngman, *Submission PR 394*, 7 December 2007.

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

80 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General). A similar description of the role of conciliation and determinations was given in Explanatory Memorandum, Privacy Bill 1988 (Cth), 3. Note determinations originally were automatically binding between parties, before the amendments made by the *Law and Justice Amendment Act 1994* (Cth) and the *Human Rights Legislation Amendment Act 1995* (Cth).

81 Rec 5–2.

complaints. It also would clarify the Commissioner's ability to conciliate a complaint at any stage after receiving it.[82]

49.61 The ALRC also recommends that the *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should clarify that the Commissioner must use reasonable attempts to conciliate a complaint where the Commissioner thinks it reasonably possible that the complaint may be conciliated successfully. This expands on the existing obligation of the Commissioner in s 27 to conciliate complaints where appropriate, and is similar to obligations of privacy commissioners under other privacy legislation.[83] The ALRC notes the concerns of the OPC in relation to the words 'all reasonable attempts', and agrees that the term 'reasonable attempts' is appropriate in this context.

49.62 In addition, the provisions should set out clearly what happens when conciliation fails. The ALRC recommends that conciliation will be taken to have failed where, in the opinion of the Commissioner, reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation. This framework adopts language from industrial relations legislation, where conciliation and arbitration are well-established practices in resolving disputes.[84] State and territory privacy legislation also provides expressly for conciliation failing or being unsuccessful.[85] This amendment would, if implemented, provide clearer parameters in which to conduct conciliation.

49.63 Finally, the ALRC recommends that the Act should be amended to provide that, where the Commissioner is of the opinion that conciliation has failed, the Commissioner must notify the complainant and respondent of this conclusion and the complainant or respondent may require that the complaint be resolved by determination.

49.64 This recommendation is analogous to the provisions in the *Information Privacy Act 2000* (Vic), where, if the Commissioner has attempted unsuccessfully to conciliate a complaint, he or she must notify the complainant and the respondent in writing, and the complainant may require the Commissioner to refer the complaint to the Victorian

---

82 Note there is precedent for a more open conciliation power in the *Anti-Discrimination Act 1977* (NSW) s 91A, which provides that the President may 'at any stage after acceptance of the complaint endeavour to resolve the complaint by conciliation'. The ability of the Commissioner to conciliate the complaint at any stage is also reflected in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–5(a).

83 See, eg, *Information Privacy Act 2000* (Vic) s 33; *Health Records Act 2001* (Vic) s 59. See also the precedent in *Industrial Relations Act 1996* (NSW) s 109.

84 See, eg, *Industrial Relations Act 1996* (NSW) ss 134–135.

85 See *Information Privacy Act 2000* (Vic) s 37; *Health Records Act 2001* (Vic) s 63; *Information Act 2002* (NT) s 111.

Civil and Administrative Tribunal for hearing.[86] It is also comparable to the approach in the *Human Rights and Equal Opportunity Commission Act 1986* (Cth) where, if the President terminates a complaint on the basis that he or she is satisfied that there is no reasonable prospect of the matter being settled by conciliation, any person affected in relation to the complaint may make an application to the Federal Court or the Federal Magistrates Court alleging unlawful discrimination by the respondent.[87] The ALRC's recommended model also is similar to the relationship between conciliation and arbitration in state industrial relations legislation.[88]

49.65 This recommendation, if implemented, should lead to an increase in the number of determinations issued by the OPC, which would help address concerns from stakeholders about the lack of jurisprudence on the *Privacy Act*.[89] The recommendation should increase public enforcement and awareness of the Act, which is consistent with Parliament's expectation that the Commissioner 'be the means by which there will be accountability to the public on the use by government of their personal information'.[90] It also is consistent with the legislative intention that determinations be issued where conciliation has failed. The presence of the power to request a determination should provide a real incentive for agencies and organisations to engage in the conciliation process, which some stakeholders suggest has been lost due to the very limited number of determinations issued. In addition, the ALRC is concerned that the conciliation process cannot properly occur under the Act where it is open to the Commissioner to close the complaint when it decides that the respondent has made an offer that adequately deals with the complaint.

49.66 Recommendation 45–13, below, will allow the Commissioner to make a determination without oral hearing where he or she believes the matter could be determined fairly on the basis of written submissions. This will mean that the determination process may be quicker and not as costly to parties and the OPC as it is under the current arrangements. It will not be as great a burden on the OPC, therefore, for a party to compel a determination where conciliation has failed.

49.67 There is some risk that providing a right to compel a determination may encourage vexatious litigants and add to the unreasonable expectations sometimes held by complainants about how a complaint will be resolved. The model recommended by the ALRC, however, incorporates adequate safeguards against vexatious and trivial conduct, as it operates only in relation to complaints that the Commissioner has not dismissed under s 41. That is, the complaint must have passed the threshold

---

86 *Information Privacy Act 2000* (Vic) s 37. See also *Health Records Act 2001* (Vic) s 63; *Information Act 2002* (NT) s 113.

87 *Human Rights and Equal Opportunity Act 1986* (Cth) ss 46PH(1)(i), 46PO.

88 See, eg, *Industrial Relations Act 1996* (NSW) s 135.

89 The ALRC considers that there is greater jurisprudential value in determinations than in case notes of conciliated complaints.

90 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General). Note this speech only refers to the government, as organisations were not covered by the *Privacy Act* when the Act was originally passed.

requirements of being in time; involving a possible breach; and not being frivolous, vexatious, misconceived or lacking in substance. The complaint, therefore, must have a degree of merit. The recommendation also requires the complainant and respondent to have made a genuine and concerted effort to conciliate the complaint.

49.68 Finally, the ALRC recommends that the Act should be amended to protect evidence produced in the conciliation process from being used in a determination hearing or later enforcement proceedings. This recommendation is based on a provision in the Victorian *Information Privacy Act*,[91] and is intended to encourage parties to engage in full and frank negotiations as part of conciliation. Where, however, the communication or evidence in issue was made in furtherance of the commission of a fraud or an offence, or in the commission of an act that would render a person liable to a civil penalty, the evidence should not be protected.[92]

49.69 Complainants should not have a right to request a determination if their complaint is dismissed. Given that many complaints are dismissed on the basis that they are trivial, frivolous, vexatious, lacking in substance or the Commissioner lacks jurisdiction, it would not be a feasible or a productive use of the OPC's resources to require a determination (potentially) in each case.

Addressing systemic issues

49.70 The ALRC recognises the need for the Commissioner to be able to prescribe remedies that address systemic issues and effect systemic changes in agencies, organisations and industries. The ALRC recommends that the Commissioner's determination powers under s 52 should be amended to empower the Commissioner to make a declaration in a determination that a respondent must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*.[93] The ability to prescribe how the respondent should act to comply with, for example, the model Uniform Privacy Principles (UPPs) should end the difficulty described by stakeholders of not knowing how to prevent future harm. It also should provide greater certainty to agencies, organisations and the public on what behaviour is consistent with the principles or regulations.[94]

49.71 While a determination may relate to an individual complaint, that individual complaint may itself be about a systemic issue. Empowering the Commissioner to

---

91 See *Information Privacy Act 2000* (Vic) s 36.

92 This exception is based on the exception to the general exclusion of evidence of settlement negotiations under s 131 of the *Evidence Act 1995* (Cth).

93 This wording is based on the compliance notice model used in other privacy legislation. See *Information Privacy Act 2000* (Vic) s 44; *Health Records Act 2001* (Vic) s 66; *Information Act 2002* (NT) s 82.

94 Greater certainty was requested by some residential tenancy database operators following the 2004 determinations: see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159.

prescribe remedies that are able to address systemic issues in the complaint-handling process allows the Commissioner to achieve maximum change from each determination.

49.72 It also should be noted that a declaration to take specified action to comply with the *Privacy Act* would be one of several declarations that the Commissioner can make as part of a determination under s 52.[95] As is the case with other determinations, it would not be binding or conclusive between parties.[96] A determination would be subject to merits review by the Administrative Appeals Tribunal (AAT).[97]

49.73 The ALRC does not agree that this recommendation is incompatible with outcomes-based or principles-based regulation. As noted in Chapter 4, a principles-based regime does not mean that agencies and organisations always will be left to find their own way of achieving compliance after an instance of non-compliance. In some instances, the particulars of the breach may demonstrate that the respondent is having trouble, either deliberately or in good faith, with finding its own way to achieving the desired outcome. In such circumstances, the appropriate enforcement response may be to prescribe the steps the respondent should take to achieve compliance with the principle. For example, the OPC would not tell a business what price it should set for access to information. It may, however, through its determination, direct an organisation to develop a price for access to information that is reasonable, having regard to whatever factors may be relevant in the circumstances.

Recommendation 49–4 The *Privacy Act* should be amended to clarify the Privacy Commissioner's functions in relation to complaint handling and the process to be followed when a complaint is received.

Recommendation 49–5 The *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should give effect to the following:

(a) If, at any stage after accepting the complaint, the Commissioner considers it reasonably possible that the complaint may be conciliated successfully, he or she must make reasonable attempts to conciliate the complaint.

---

95 Other declarations that may be made under s 52(1) include declarations that the complainant is entitled to compensation for any loss or damage, or a declaration that the respondent should perform any reasonable act to redress any loss or damage suffered by the complainant.

96 See s 52(1B).

97 See Rec 49–7. The need for an appeal process was noted in one submission: Australian Federal Police, *Submission PR 545*, 24 December 2007.

(b) Where, in the opinion of the Commissioner, reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination.

(c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.

(d) Subparagraph (c) does not apply where the communication was made in furtherance of the commission of a fraud or an offence, or in the commission of an act that would render a person liable to a civil penalty.

Recommendation 49–6 The *Privacy Act* should be amended to empower the Privacy Commissioner, in a determination, to prescribe the steps that an agency or respondent must take to ensure compliance with the Act.

Accountability and transparency

Background

49.74 A number of stakeholders to this Inquiry submitted that transparency and accountability in complaint handling under the *Privacy Act* should be improved. Two methods of improving transparency and accountability are merits review of the Commissioner's determinations and providing more guidance on the OPC's complaint-handling policies and procedures.

Merits review

Background

49.75 The right to merits review of determinations made by the Commissioner is limited to where the respondent is an agency, and is available only in relation to the Commissioner's decision to include or not include a declaration for compensation or costs.[98] There is no right of appeal to the AAT in respect of determinations against organisations or determinations dismissing a complaint.

98 *Privacy Act 1988* (Cth) s 61.

49.76 Some stakeholders making submissions to the OPC Review expressed the view that the narrowness of merits review available under the *Privacy Act* is one factor that prevents there being a useful legal jurisprudence on the Act on which people can rely.[99] It was suggested that the existing provisions were unfair to complainants because, while respondents have a de facto right to have the case heard afresh by refusing to comply with a determination and waiting for the Commissioner or complainant to enforce it in court, this strategy is not available to an aggrieved complainant.[100] The OPC Review concluded that the lack of merits review of determinations was out of step with the position applying to other government authorities and recommended that the Australian Government amend the Act 'to give complainants and respondents a right to have the merits of complaint decisions made by the Commissioner reviewed'.[101]

Submissions and consultations

49.77 In DP 72, the ALRC identified strong support in submissions and consultations for a right to merits review of all complaint determinations.[102] To increase transparency and accountability, and to facilitate the growth of more jurisprudence on the *Privacy Act*, the ALRC proposed that the Act be amended to provide for merits review of all decisions made by the Commissioner under s 52.[103]

49.78 Almost all of the stakeholders that commented on this proposal expressed support for it, including the OPC.[104] PIAC expressed the view that restrictions on the ability of parties to seek merits review in the AAT 'have long been a major deficiency in the *Privacy Act*'.[105] The AAT submitted that it would not oppose conferral of the

---

99 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 137–138.

100 Ibid, 138–139. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

101 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 153, rec 40.

102 Queensland Government, *Submission PR 242,* 15 March 2007; Legal Aid Queensland, *Submission PR 212,* 27 February 2007; Privacy NSW, *Submission PR 193,* 15 February 2007; Telstra, *Submission PR 185,* 9 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; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988,* 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

103 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–7.

104 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556,* 7 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; 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; Australasian Compliance Institute, *Submission PR 419,* 7 December 2007; P Youngman, *Submission PR 394,* 7 December 2007.

105 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

proposed jurisdiction, although it noted that generally its jurisdiction to review decisions arising from complaints involved decisions imposing sanctions.[106]

ALRC's view

49.79 The current right to merits review of determinations are not sufficient. To increase transparency and accountability, the *Privacy Act* should be amended to provide for merits review of all decisions made by the Commissioner under s 52. Implementation of this recommendation will have the ancillary benefit of facilitating the growth of more jurisprudence on the Act.

Recommendation 49–7 The *Privacy Act* should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner.

Complaint-handling policies and procedures

Background

49.80 Another method of increasing transparency and accountability in the OPC's processes and decision making is by publishing clear policies and procedures that outline how the OPC deals with complaints, and by publishing case notes.

49.81 Submissions from stakeholders calling for the OPC to produce a comprehensive manual on its complaint-resolution policies and procedures, in order to shed more light on the way it handles complaints, were considered in the OPC Review.[107] The OPC Review recognised that greater transparency was likely to benefit both complainants and respondents and would increase scrutiny of the OPC's decisions. It found, however, that 'it does not appear to be common practice for regulators to publish manuals which set out in great detail their complaint processes'.[108]

49.82 Case notes can help to make the OPC's handling of complaints more transparent, which in turn improves accountability, by providing examples of how the principles have been interpreted and applied in practice. The OPC publishes case notes that describe the issues in, and outcomes of, selected complaints and has stated that, by providing this insight into how the privacy principles are being applied, the Commissioner aims to 'ensure the Office is accountable and transparent in its

106 Administrative Appeals Tribunal, *Submission PR 481*, 17 December 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), 137, 142, 151.
108 Ibid, 151.

processes and decision making'.[109] Case notes also play an important role 'to assist individuals, organisations and agencies in deciding whether to pursue a complaint, or to decide if personal information is being handled appropriately', and 'to encourage good privacy practices and compliance with the *Privacy Act'*.[110]

Submissions and consultations

49.83 In DP 72, the ALRC identified concern about the lack of transparency and accountability in the OPC's complaint-handling procedures.[111] In particular, stakeholders commented on the lack of transparency about complaint resolutions and the remedies being granted by the OPC,[112] and the lack of transparency around how the OPC screens complaints in the initial stages.[113] To remedy this situation, the ALRC proposed that the OPC should prepare and publish a document setting out its complaint-handling policies and procedures.[114]

49.84 Stakeholders supported the production of such a document.[115] A number of stakeholders expressed a view as to the issues that should be addressed. These included that the document should:

- be clear, able to be comprehended easily and available in different languages;[116]
- be widely accessible and subject to periodic review;[117]

---

109 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 58. See Office of the Privacy Commissioner, *Complaint Case Notes, Summaries and Determinations* (2007) <www.privacy.gov.au/act/casenotes/index.html> at 15 May 2008.

110 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [3.5]. See Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2, 2.

111 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; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

112 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; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988,* 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

113 AAMI, *Submission PR 147,* 29 January 2007.

114 Australian Law Reform Commission, *Review of Australian Privacy Law,* DP 72 (2007), Proposal 45–8.

115 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008; Australian Government Centrelink, *Submission PR 555,* 21 December 2007; 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; GE Money Australia, *Submission PR 537,* 21 December 2007; Medicare Australia, *Submission PR 534,* 21 December 2007; Australian Lawyers Alliance, *Submission PR 528,* 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007.

116 Law Society of New South Wales, *Submission PR 443,* 10 December 2007.

117 Ibid.

- include guidelines about confidentiality during the investigation and conciliation process;[118] and

- specify timeframes for the resolution of disputes, including for the various steps of the process. [119]

49.85 The Cyberspace Law and Policy Centre submitted that, as well as a complaint-handling policy, the OPC should continue to improve its reporting of how complaints have been handled and settled—including statistics of the remedies obtained (including the number of cases in which compensation was paid and the amounts).[120]

49.86 Youthlaw suggested that the OPC should consider new approaches to make complaint mechanisms more 'user-friendly' for young people. These included:

- setting up a specific contact/advice point for young people to access if they believe their rights to privacy may have been breached;
- better resourcing and funding of youth specific legal services to assist young people to utilise existing complaints mechanisms;
- training to youth workers regarding privacy and assisting young people to protect their privacy or provide outreach workers from the Privacy Commission to deliver information to youth services or schools.[121]

ALRC's view

49.87 A valuable way of increasing transparency in complaint handling under the *Privacy Act* would be for the OPC to prepare and publish a document setting out its complaint-handling policies and procedures. This document could draw on existing resources and publications of the OPC, such as information included in the 'Privacy Complaints' section on the OPC website and in Information Sheet 13, which sets out the Commissioner's approach to promoting compliance with the *Privacy Act*.[122] The recommended document also could include the OPC's determination policy.[123] The guide should be easy to understand and readily accessible, and should indicate the timeframes involved in the complaint-resolution process, where possible.

---

118 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
119 Ibid.
120 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
121 Youthlaw, *Submission PR 390*, 6 December 2007.
122 See Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007; Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001).
123 Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2.

49.88 Consolidating this information into one document should increase the accessibility and transparency of the complaint-handling process. It also would make a useful resource for agencies, organisations and individuals.

49.89 In Chapter 67, the ALRC recommends that the OPC should develop and publish educational material about privacy issues aimed at children and young people.[124] This material should include information about the role of the OPC and its complaint-handling processes in an accessible format.

Recommendation 49–8 The Office of the Privacy Commissioner should develop and publish a document setting out its complaint-handling policies and procedures.

Other issues in the complaint-handling process

Background

49.90 In addition to general issues about investigating and resolving complaints under the *Privacy Act*, stakeholders raised a number of concerns relating to specific provisions in the Act. These included those provisions dealing with representative complaints, preliminary inquiries and the conduct of investigations.

Representative complaints

49.91 The *Privacy Act* allows for the making of representative complaints, whereby one of a class of two or more individuals makes a complaint on behalf of all the individuals in the class.[125] A representative complaint can be lodged under s 36 if the class members have complaints against the same person; all the complaints are in respect of, or arise out of, the same or related circumstances; and all the complaints give rise to a substantial common issue of law or fact.[126]

49.92 The Commissioner has power to determine that a complaint should no longer be treated as a representative complaint, and may turn an individual complaint into a representative complaint.[127] The Commissioner also can replace the complainant with another class member and a class member can withdraw from a representative complaint at any time before the Commissioner begins to hold an inquiry into the complaint. Under ss 38(3) and 39 of the *Privacy Act*, representative complaints can be lodged without the consent of class members and a person who is a class member for a

124 Rec 67–2.
125 *Privacy Act 1988* (Cth) s 36(2).
126 Ibid s 38(1).
127 Ibid ss 38A, 38C.

representative complaint is not entitled to lodge a complaint in respect of the same subject matter.[128]

Submissions and consultations

49.93 In DP 72, the ALRC identified a number of concerns raised by the OPC in relation to the procedures for making and pursuing representative complaints. One such concern was that an individual's capacity to make an individual complaint could be removed without his or her knowledge or agreement, by virtue of the combination of ss 38(3) and 39 of the *Privacy Act*.[129]

49.94 To address this issue, the ALRC proposed that the *Privacy Act* should be amended to allow a class member of a representative complaint to withdraw from the complaint at any time if the class member has not consented to be a class member.[130]

49.95 The Australian Privacy Foundation submitted that, while there was no evidence of this problem occurring in practice, individuals should not be able to be named as parties to a complaint 'against their will'.[131] This view was shared by a number of other stakeholders.[132]

ALRC's view

49.96 The *Privacy Act* should be amended to allow a class member of a representative complaint to withdraw from the complaint at any time if the class member has not consented to be a class member. This would address the issue that an individual's right to lodge a complaint can be removed by circumstances beyond his or her knowledge or control. The *Human Rights and Equal Opportunity Commission Act* contains a similar provision.[133]

49.97 In relation to the issue of standing, s 38A gives the Commissioner a broad discretion to determine that a complaint should not continue as a representative complaint when he or she is satisfied that it is in the interests of justice to do so. Reasons for making such a determination include that the complaint was not brought in good faith as a representative complaint, or where it is otherwise inappropriate that the complaints be pursued by means of a representative complaint.[134] These powers

---

128 Ibid ss 38, 39.
129 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
130 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–9.
131 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
132 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.
133 *Human Rights and Equal Opportunity Act 1986* (Cth) s 46PC.
134 *Privacy Act 1988* (Cth) s 38A(2)(c), (d).

provide the OPC with adequate discretion to cease handling a complaint as a representative complaint where it was brought by a person with no standing.[135]

Recommendation 49–9 The *Privacy Act* should be amended to allow a class member to withdraw from a representative complaint at any time if the class member has not consented to be a class member.

Preliminary inquiries

49.98 Under s 42 of the *Privacy Act*, where a complaint is made to, or accepted by, the Commissioner, he or she has the power to make preliminary inquiries of the respondent. The power is limited by its purpose, which is to determine whether the Commissioner has power to investigate the matter complained about, or whether the Commissioner may exercise his or her discretion not to investigate the matter.

49.99 In DP 72, the ALRC proposed adoption of a suggestion of the OPC that the Commissioner should be given a specific power to contact third parties when undertaking preliminary inquiries into a complaint.[136] The OPC suggested this was particularly relevant when the complaint relates to a disputed credit default, in which case it is usually relevant to the assessment of the case for the OPC to seek a copy of the individual's credit information file. The OPC submitted that, while it has the power to do anything 'incidental or conducive to the performance of any of the Commissioner's other functions',[137] it would be appropriate to have a specific power to contact third parties in these circumstances.[138]

Submissions and consultations

49.100 Significant support was received for this proposal.[139] Some stakeholders commented that the Commissioner should have the appropriate authority to obtain all the relevant facts as early as possible in the complaint-handling process.[140]

49.101 Concern was expressed, however, by other stakeholders that the proposal could affect the confidentiality of the investigation. The Australian Direct Marketing

---

135 See also Australian Law Reform Commission, *Beyond the Door-Keeper: Standing to Sue for Public Remedies*, ALRC 78 (1996).

136 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–10.

137 *Privacy Act 1988* (Cth) s 27(1)(s).

138 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

139 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

140 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

Association stated that 'the ability to disclose that an investigation is being undertaken to a third party may impugn the reputation and standing of the respondent'.[141]

49.102 The Law Society of New South Wales, while offering qualified support for the proposal, noted that inquiries of third parties must not jeopardise the complainant's case and the complainant and the respondent should be informed of the names of the persons or entities the Commissioner intends to contact. The Law Society submitted that parties should be allowed to object to the Commissioner contacting third parties.[142] One stakeholder also was concerned that if the Commissioner was able to make inquiries of third parties, 'the model for complaint determination will move from an adversarial to an inquisitorial model'.[143]

ALRC's view

49.103 While other similar regulatory agencies, such as the Commonwealth Ombudsman, do not have the power to contact third parties during preliminary inquiries, they do have the same general powers as the Privacy Commissioner to undertake investigations and question third parties as required to perform their functions.

49.104 Section 42 of the *Privacy Act* should be amended to allow the Commissioner to contact third parties at the preliminary inquiry stage. While it is possible that a similar result could be achieved through the Commissioner's ancillary function, it would be clearer and more transparent if the section itself provided specifically that the Commissioner has the ability to make inquiries of third parties. Any such inquiries should be made on a confidential basis. In the interests of fairness and transparency, the complainant should be informed of the Commissioner's intention to make preliminary inquiries of a third party.

49.105 This amendment was sought from the OPC mostly to address issues in the context of credit reporting. While the ALRC acknowledges that the OPC could request the individual's credit file directly from the individual, this recommendation also would help reduce delays in addressing complaints in the credit reporting context.

---

141 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007. PIAC also noted that third parties should be made aware of the importance of confidentiality in the investigation and conciliation process: Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

142 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

143 Confidential, *Submission PR 536*, 21 December 2007.

Recommendation 49–10 The *Privacy Act* should be amended to permit the Privacy Commissioner, in accepting a complaint or determining whether the Commissioner has the power to accept a complaint, to make preliminary inquiries of third parties as well as the respondent. The Privacy Commissioner should be required to inform the complainant that he or she intends to make inquiries of a third party.

Ceasing investigations if certain offences have been committed

49.106 If the Commissioner forms the opinion, in the course of an investigation, that a 'credit reporting offence' or 'tax file number offence' has been committed, he or she must inform the Commissioner of Police or the Commonwealth Director of Public Prosecutions (CDPP), and is to discontinue the investigation except to the extent that it concerns matters unconnected with the alleged offence. The Commissioner may continue with the investigation upon receiving a notice from the Commissioner of Police or the CDPP indicating that the matter will not, or will no longer be, the subject of proceedings for an offence.[144]

Submissions and consultations

49.107 In DP 72, the ALRC identified the concerns of the OPC about delays caused by the requirement to refer matters to the Australian Federal Police (AFP) for investigation. As the OPC's investigation is suspended while the AFP decides whether to investigate, this can cause delay in resolving the complaint. The OPC suggested that a way to alleviate these problems would be for the 'offence provisions to set a higher test than the test for an interference with privacy under the *Privacy Act*', thereby giving the OPC a discretion not to refer a matter to the AFP where the conduct was not serious or caused no harm. While most offence provisions already set a higher test than for an interference with privacy (see, for example, s 18R), the exception is the tax file number offence under s 8WB of *Taxation Administration Act 1953* (Cth).[145]

ALRC's view

49.108 While noting the OPC's concerns, the ALRC does not recommend that the *Privacy Act* be amended to set a higher test for referral of credit reporting or tax file number offences to the AFP. Although the operation of this provision can cause delays to the OPC's investigation, the referral of offences to the AFP and the DPP is part of the broader prosecution policy of the Australian Government.[146] The ALRC also has

---

144 *Privacy Act 1988* (Cth) s 49. An example of the operation of this provision is provided in *F and G v Taxation Accountant* [2006] PrivCmrA 6.

145 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

146 In particular, see Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* (1992). The AFP also prioritises matters for investigations pursuant to its Australian Federal Police, *Case Categorisation and Prioritisation Model* (2006). Section 8WB of the *Taxation Administration Act* is currently under review by the Australian Government Treasury as part of the

recommended that the *Privacy Act* should be amended to remove the credit reporting offences and allow a civil penalty to be imposed.[147] This would limit the OPC's concerns only to tax file number offences.

Conduct of investigations

49.109 The *Privacy Act* outlines how an investigation is to be conducted. As a general rule, an investigation is to be 'conducted in private but otherwise in such manner as the Commissioner thinks fit'.[148] The Commissioner must inform parties when an investigation commences or ceases.[149] For the purposes of performing the Commissioner's functions relating to a complaint (except a complaint under the NPPs or a code complaint accepted under s 40(1B)), the Commissioner can compel the complainant, respondent and any other relevant person to attend a conference.[150] The Commissioner also has the power, subject to certain limitations, to obtain information and documents from persons, and make inquiries of persons or examine witnesses on oath or affirmation.[151]

49.110 In addition to these requirements, the *Privacy Act* requires that complainants and respondents be given the opportunity to appear before the Commissioner in certain circumstances. In particular, the Commissioner must not make a finding under s 52 that is adverse to a complainant or respondent unless the Commissioner has afforded the complainant or respondent an opportunity to appear before the Commissioner and to make submissions orally, in writing, or both, in relation to the matter to which the investigation relates.[152] This requirement reflects the 'hearing rule' which, in the context of administrative decision making, is the common law rule that a statutory authority having power to affect the rights of a person is bound to afford the person a hearing before exercising the power.[153]

49.111 The rules of natural justice, including the hearing rule, can be modified or abrogated by statute.[154] For example, the *Social Security (Administration) Act 1999* (Cth) provides that a party to a merits review of a decision before the Social Security Appeals Tribunal may make oral or written submissions, or both.[155] The Executive

---

inquiry into secrecy and disclosure provisions in Australian taxation law: see Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006).

147 Rec 59–9. See also Rec 50–2.

148 *Privacy Act 1988* (Cth) s 43(2).

149 Ibid ss 43(1), 48.

150 Ibid s 46(1). It is an offence to fail to attend such a conference as required by the Commissioner: *Privacy Act 1988* (Cth) s 46(2).

151 *Privacy Act 1988* (Cth) ss 44–46. It is an offence not to comply with the Commissioner's directions: *Privacy Act 1988* (Cth) ss 46(2), 65–66.

152 *Privacy Act 1988* (Cth) s 43(4)–(5).

153 See R Creyke and J McMillan, *Control of Government Action: Text, Cases & Commentary* (2005); *Twist v Council of the Municipality of Randwick* (1976) 136 CLR 106, 110.

154 *Kioa v Minister for Immigration and Ethnic Affairs* (1985) 159 CLR 550.

155 *Social Security (Administration) Act 1999* (Cth) s 161.

Director of the Social Security Appeals Tribunal may direct, however, that a hearing be conducted without oral submissions from the parties if: the Executive Director considers that the review hearing could be determined fairly on the basis of written submissions by the parties; and all the parties to the review consent to the hearing being conducted without oral submissions.[156]

49.112 The *Administrative Appeals Tribunal Act 1975* (Cth) provides that a matter may be dealt with by considering documents or other material lodged with or provided to the AAT—without holding a hearing—if it appears to the AAT that the issues for determination on the review of a decision can 'be adequately determined in the absence of parties; and the parties consent to the review being determined without a hearing'.[157]

49.113 In DP 72, the ALRC identified several issues raised by the OPC in relation to the Commissioner's powers to conduct investigations. These included the OPC's comments that the powers in ss 46 and 47 should be clarified to make it clear that they relate to a compulsory *conciliation* conference, and that the Commissioner should be empowered to compel parties to an NPP complaint—as well as other types of complaints—to attend a compulsory conference. The OPC also commented on the restrictions in s 69, in relation to personal information and documents that can be furnished or produced to the Commissioner during the investigation of a privacy complaint. Section 69 of the Act prevents people giving the Commissioner information generated for the purposes of taxation law or a law relating to the census or statistics, unless it relates to an individual who has made a complaint. Secondly, it sets out 'very broad restrictions on the provision of information about an individual other than the complainant to the Commissioner', requiring that such information can be provided only with the individual's consent.

49.114 Finally, the OPC raised the issue of enabling the Commissioner to make a determination 'on the papers'—without holding a hearing—in certain circumstances.[158]

Submissions and consultations

49.115 In DP 72, the ALRC made several proposals to address these concerns and increase the Commissioner's investigatory powers. In particular, the ALRC proposed that:

- s 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to a complaint, and any other relevant person, to attend a compulsory conference;[159]

---

156 Ibid s 162.

157 *Administrative Appeals Tribunal Act 1975* (Cth) s 34J. Note that s 76 of the *Administrative Decisions Tribunal Act 1997* (NSW) gives the Administrative Decisions Tribunal power to determine proceedings without holding a hearing if the Tribunal believes the issues can be adequately determined in the absence of the parties.

158 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

159 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 45–11.

- s 69(1) and (2) of the *Privacy Act* should be deleted, which would allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant;[160] and

- the *Privacy Act* should be amended to provide that the Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties, if the Commissioner considers that the matter could be determined fairly on the basis of written submissions by the parties and the complainant and respondent consent to the matter being determined without oral submissions.[161]

49.116 The proposal to extend the Commissioner's power to compel a party to attend a compulsory conference to private sector complaints was supported in submissions by a number of stakeholders.[162]

49.117 The proposal to allow the Commissioner to collect personal information about an individual who is not the complainant also was generally supported.[163] Medicare Australia submitted that this would bring the *Privacy Act* in line with other legislation.[164] The Law Society of New South Wales noted, however, that privacy protection must be given to the third party in relation to that information.[165] Centrelink expressed concern that allowing the Commissioner to make direct approaches to other individuals who are not the complainant may have an impact on the investigation of complaints by the agency itself and duplicate resources.[166] The Australian Direct Marketing Association (ADMA) submitted that allowing the Commissioner to collect information about third parties may be open to abuse and impugn the reputation and standing of the respondent.[167]

---

160 Ibid, Proposal 45–12.
161 Ibid, Proposal 45–13.
162 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; GE Money Australia, *Submission PR 537,* 21 December 2007; Medicare Australia, *Submission PR 534,* 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.
163 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; GE Money Australia, *Submission PR 537,* 21 December 2007; Medicare Australia, *Submission PR 534,* 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.
164 Medicare Australia, *Submission PR 534,* 21 December 2007.
165 Law Society of New South Wales, *Submission PR 443,* 10 December 2007.
166 Australian Government Centrelink, *Submission PR 555,* 21 December 2007.
167 Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007.

49.118 The Law Society of New South Wales supported the proposal to allow the Commissioner to conduct a hearing for determination based on written submissions with the consent of the parties. It noted that this process could obviate the need for a formal hearing and assist in the early resolution of disputes.[168] The proposal also was supported by a number of privacy advocates and other stakeholders.[169]

49.119 The OPC agreed with the general premise of the proposal, but submitted that the Commissioner should have the power to direct that a hearing for a determination be conducted without oral submissions from the parties where he or she considers that the matter could be determined fairly on the basis of written submissions from the parties, even where the parties had not consented to this process. In the OPC's view, this approach would give the Commissioner greater flexibility to conduct a hearing in a fair and efficient manner. The OPC argued that:

> Were the Commissioner to consider that the matter could be determined fairly on the basis of written submissions for the parties, there would be no need to seek consent of the parties.[170]

ALRC's view

49.120 In relation to compulsory conferences, the Explanatory Memorandum for the Privacy Bill made it clear that ss 46 and 47 were intended to empower the Commissioner to 'direct persons to attend a compulsory conference in order to attempt a settlement of a complaint'.[171] The term 'compulsory conference' is used only in the section headings for ss 46 and 47. It is not necessary for the word 'conciliation' to be included in the section heading.[172] The OPC, however, could clarify the role of conferences in the conciliation process in the document setting out its complaint-handling policies and procedures.[173]

49.121 The power to compel parties to attend a compulsory conference should extend to where the complaint is a complaint about an organisation under the UPPs,[174] or a code complaint accepted under s 40(1B). Conciliation conferences are an important part of the conciliation process, and the Commissioner's powers to resolve complaints should be consistent across all types of complaints. There appears to be no policy reason why the Commissioner should not have the same power to deal with private sector complaints as with complaints concerning agencies.

---

168 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

169 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. The proposal also was supported by the Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007 and Veda Advantage, *Submission PR 498*, 20 December 2007.

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

171 Explanatory Memorandum, Privacy Bill 1988 (Cth). This interpretation of compulsory conferences also is consistent with *Human Rights and Equal Opportunity Act 1986* (Cth) ss 46PJ(1), 46PF(1).

172 Under the *Acts Interpretation Act 1901* (Cth) s 13(3), a section heading is not considered to be part of the Act, meaning that the heading cannot be used in interpreting the meaning of a section.

173 Rec 49–8.

174 If Rec 18–2 is adopted, there will be a single set of privacy principles—the model UPPs.

49.122 The restrictions in s 69(1)–(2) on the Commissioner's ability to collect third party information in the process of investigating a complaint should be removed. These restrictions may fetter the ability of the Commissioner to resolve complaints efficiently and effectively, and are inconsistent with provisions applying to other regulators.[175] The ALRC also notes that the OPC is subject to secrecy provisions in s 96 of the *Privacy Act*, which make it an offence for the Commissioner or a member of his or her staff (present and past) to disclose, use or make a record of information acquired about a person in the performance of that role, other than to do something permitted or required by the *Privacy Act*.[176] These provisions provide protection for any information collected in an investigation.

49.123 In relation to the hearing requirements before a determination is made, the ALRC recommends that the *Privacy Act* should be amended to give the Commissioner flexibility to make determinations on the basis of written submissions in certain circumstances. The ALRC recognises that there may be situations where a determination could be made fairly and efficiently without parties appearing before the Commissioner to make oral submissions. The ALRC also recognises that Recommendation 49–5—that complainants and respondents be given the right, in certain circumstances, to require that a complaint be resolved by a determination—would, if implemented, give rise to a consequent right for the complainant or respondent to appear before the Commissioner before a determination is made. The combination of that recommendation and the current provision could increase the number of hearings held by the Commissioner, which may have significant resource implications for the OPC. There is merit, therefore, in giving the Commissioner greater flexibility to make determinations on the basis of written submissions.

49.124 There are several options to allow for determinations on the papers. The first is to remove the automatic right to appear before the Commissioner and instead give the Commissioner the discretion to provide a party with an opportunity to appear before him or her where the Commissioner considers that it would be fair in all the circumstances to make a determination based on written submissions. Under s 76 of the *Administrative Decisions Tribunal Act 1997* (NSW), the Administrative Decisions Tribunal is given the power to determine proceedings without holding a hearing if the Tribunal believes the issues can be adequately determined in the absence of the parties.

49.125 The second option is to retain the current right to appear before the Commissioner to make oral or written submissions, but to provide explicitly that a hearing can be conducted on the basis of written submissions only where the parties

---

175 For example, there is no equivalent provision in the *Human Rights and Equal Opportunity Act 1986* (Cth) or other state or territory privacy legislation.

176 *Privacy Act 1988* (Cth) s 96(1), (3). The offence is punishable by a penalty of $5,000 or imprisonment for one year, or both. Note that the OPC released its privacy policy (which sets out its personal information handling practices) in August 2006: Office of the Privacy Commissioner, *Privacy Policy* (2006).

agree. This is the approach taken in the *Social Security (Administration) Act* and was the ALRC's preferred option in DP 72.

49.126 Since DP 72, the ALRC has formed the view that fairness to the parties is a more important concern than consent. Parties may consent to a hearing on the papers because they believe it will be easier or cheaper. This may not always produce a fair result however, particularly where a party has language, literacy or capacity issues that hinder his or her ability to present a case entirely in a written submission. It is appropriate for the Commissioner to determine when a matter could be determined fairly on the basis of written submissions by the parties. If one party did not consider that he or she could put his or her case adequately in a written submission, then the OPC should take this into account.

49.127 The ALRC therefore supports the view of the OPC that it should be granted the power to direct that a hearing may be conducted without oral submissions from the parties if the Privacy Commissioner is satisfied that the matter could be determined fairly on the basis of written submissions. The ALRC notes that determinations are reviewable by the AAT, so parties will have an avenue of appeal in the event that they dispute a decision of the Commissioner.

49.128 The document containing the OPC's complaint-handling policies and procedures[177] should set out the factors the OPC will consider in deciding whether it is fair to determine the matter based on written submissions. These factors should include (but are not limited to): the relative ability of the parties to communicate effectively in writing; whether the parties have had access to legal advice; the complexity of the issues; the amount of information or evidence required from third parties; and whether it would be in the interests of fairness for the matter to be resolved without an oral hearing.

Recommendation 49–11 Section 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to a complaint, and any other relevant person, to attend a compulsory conference.

Recommendation 49–12 The *Privacy Act* should be amended to allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant.

177 Rec 49–8.

Recommendation 49–13 The *Privacy Act* should be amended to provide that the Privacy Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties if the Privacy Commissioner is satisfied that the matter could be determined fairly on the basis of written submissions by the parties.

50. Enforcing the *Privacy Act*

Contents

Introduction

50.1 The Office of the Privacy Commissioner (OPC) is responsible for enforcing compliance with the *Privacy Act 1988* (Cth). This involves investigating instances of non-compliance by agencies and organisations and prescribing remedies to redress non-compliance. While Chapter 49 examines the Privacy Commissioner's powers to investigate and resolve privacy complaints, this chapter considers the Commissioner's powers to investigate an act or practice on his or her own motion. It also considers the Commissioner's power to enforce complaint determinations, report on certain activities and apply for injunctions. Lastly, the chapter recommends other enforcement mechanisms that should be introduced into the Act.

Enforcing 'own motion' investigations

Background

50.2 In addition to the Commissioner's power to investigate an act or practice when a complaint has been made, the Commissioner also can investigate an act or practice on his or her own motion where the Commissioner considers it desirable that the act or practice be investigated.[1] Own motion investigations are used by the OPC where it becomes aware of matters that may involve interferences with privacy through media coverage, calls to the Privacy Enquiries line, or individuals writing to the OPC.[2]

Remedies following own motion investigations

50.3 The Commissioner can report to the Minister on own motion investigations made in relation to the acts and practices of agencies, file number recipients, credit reporting agencies or credit providers. Section 30 of the Act provides that, where the Commissioner has investigated an act or practice without a complaint having been made under s 36, the Commissioner may report to the Minister about the act or practice investigated and must report where the:

- Minister directs the Commissioner to do so; or

- Commissioner thinks the act or practice investigated is an interference with an individual's privacy and the Commissioner has not considered it appropriate to endeavour to settle the matter, or has tried to settle the matter without success.[3]

50.4 Section 30(6) of the Act specifies that these reporting obligations do not apply to a complaint made under s 36 in relation to an act or practice of an organisation or a complaint accepted under s 40(1B). The purpose of this subsection was said to be 'to clarify that there is no requirement to report to the Minister following investigations conducted by the Privacy Commissioner into the acts or practices of organisations'.[4]

50.5 The OPC stated in its Annual Report for 2006–07 that, in the majority of own motion investigations in which it found allegations to be substantiated, the respondent dealt with the issues of concern either on its own initiative or following the OPC's suggestions. The types of action taken included apologies, retrieval and appropriate disposal of records, and change in procedures.[5]

---

1 *Privacy Act 1988* (Cth) s 40.

2 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [3.4.1]. The Annual Report provides examples of situations investigated by the OPC on its own motion.

3 *Privacy Act 1988* (Cth) s 30(1). As at May 2008, the relevant Minister is the Cabinet Secretary.

4 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 107.

5 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [3.4.2].

50.6 The inability of the Commissioner to enforce remedies following an own motion investigation was commented on by stakeholders in the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) and the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Senate Committee privacy inquiry). In the former, stakeholders submitted that a wider power of enforcement should be conferred on the Commissioner. It was suggested that the Commissioner should 'be able to enforce any directions given in relation to findings after an own motion investigation', ensuring that 'light handed' measures taken by the Commissioner have the 'weight of possible further action attached to them'.[6]

50.7 In the OPC Review, the OPC acknowledged that it had 'experienced some difficulties' in dealing with potential privacy breaches where there was no individual complainant and where the respondent was not cooperative.[7] It recommended that the Australian Government consider amending the *Privacy Act* to 'provide for enforceable remedies following own motion investigations where the Commissioner finds a breach of the National Privacy Principles' (NPPs).[8] The Australian Government agreed with this recommendation.[9]

Submissions and consultations

50.8 In the Discussion Paper *Review of Australian Privacy Law* (DP 72), the ALRC identified support in submissions and consultations for the Commissioner's power to conduct own motion investigations as a means of addressing systemic issues. Several stakeholders reiterated the need for the Commissioner to have the power to enforce remedies following own motion investigations where the Commissioner finds that there has been a breach of the privacy principles.[10]

50.9 In response to these concerns, the ALRC proposed in DP 72 that the Commissioner be empowered to issue a notice to comply following an own motion investigation. In the notice, the Commissioner could determine that the agency or organisation has engaged in conduct constituting an interference with the privacy of an

---

6 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 145. See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 146.

7 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 155.

8 Ibid, rec 44. See also Ibid, 157.

9 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), [Item 44].

10 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Privacy NSW, *Submission PR 193*, 15 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

individual and could prescribe that the agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the Act.[11]

50.10 The OPC was supportive of the proposed amendments to increase its powers to take action following an own motion investigation.[12] Other stakeholders also expressed their support.[13] The Public Interest Advocacy Centre (PIAC), for example, stated that:

> To date, own-motion investigations have had limited value as a compliance tool because of the Commissioner's inability to enforce remedies following such investigations. The proposed amendments will greatly enhance the ability of the Commissioner to address systemic interferences with privacy.[14]

50.11 The Federation of Community Legal Centres also supported the proposal. It stated that 'a range of compliance strategies with an associated hierarchy of enforcement powers and consequences is appropriate to the modern complexities of privacy issues in Australia'.[15]

50.12 Some stakeholders argued that there also should be greater transparency in the reporting of results of own motion investigations. PIAC and the Cyberspace Law and Policy Centre submitted that there should be a requirement that reports on own motion investigations be made public, either through reporting in OPC case notes or in reports to Parliament.[16] The view was also put that there should be procedures to allow privacy and consumer groups to intervene in own motion investigations where appropriate.[17]

50.13 Other stakeholders considered the existing enforcement powers of the Commissioner to be adequate.[18] One stakeholder suggested that there was no evidence to suggest that there is widespread non-compliance with the Act or any need to change the enforcement approach. It its view, most breaches of the Act are inadvertent, and the

---

11 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 46–1.

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

13 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. This proposal was also supported by Privacy NSW: Privacy NSW, *Submission PR 468*, 14 December 2007.

14 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

15 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007. Other stakeholders who supported the proposal included: Veda Advantage, *Submission PR 498*, 20 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

16 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

17 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

18 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

fact that penalties have rarely been used is 'indicative of the fact that penalties are not required'.[19]

ALRC's view

50.14 Own motion investigations provide a valuable tool for the Commissioner to investigate allegations of non-compliance that come to light via means other than a complaint being lodged. In order to make such investigations effective as a compliance tool, however, it is important that the Commissioner have adequate means to enforce remedies where he or she finds a breach of the NPPs, the Information Privacy Principles (IPPs)[20] or other provisions in the *Privacy Act*.

50.15 Accordingly, the *Privacy Act* should be amended to allow the Commissioner to issue a notice to comply following an own motion investigation. The Commissioner should be empowered to determine in the notice that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual. Consistently with the ALRC's recommendation in relation to determinations,[21] the Commissioner also should be empowered to prescribe in the notice that the agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the Act.[22]

50.16 As with determinations, the notice should be enforceable by proceedings in the Federal Court or Federal Magistrates Court.[23] The *Privacy Act* should be amended to include a mechanism similar to that under s 55A of the Act where the complainant, the Commissioner or an adjudicator under a code may commence court proceedings for an order to enforce a determination. Unlike in the case of determinations, however, the ALRC does not recommend that there be merits review of a notice to comply issued by the Commissioner. If the respondent in a notice to comply contests the Commissioner's findings or the actions prescribed in the notice, the respondent could choose not to comply with the notice and wait for the Commissioner to enforce it in the Federal Court by way of a hearing de novo.

50.17 The ALRC agrees that the OPC's reporting of own motion investigations could be improved. In its 2006–07 Annual Report, the OPC reported it received 55 new matters and 'took steps to contact the organisation in about 85% of cases'.[24]

---

19 Confidential, *Submission PR 536*, 21 December 2007.

20 If Rec 18–2 is adopted, there will be a single set of privacy principles—the model Unified Privacy Principles (UPPs).

21 Rec 49–7.

22 The proposed wording for this power is based on the compliance notice model used in other privacy legislation: see *Information Privacy Act 2000* (Vic) s 44; *Health Records Act 2001* (Vic) s 66; *Information Act 2002* (NT) s 82.

23 Enforcement of determinations is discussed further below.

24 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), [3.4.1].

Summaries of some of the allegations are provided, but not specific details of the outcome of the investigations. The OPC should make its reporting on own motion investigations more comprehensive. If Recommendation 50–1 is implemented, this reporting should include when a notice to comply was issued, and any proceedings that were commenced for enforcement of a notice.

Recommendation 50–1 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) issue a notice to comply to an agency or organisation following an own motion investigation, where the Commissioner determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual;

(b) prescribe in the notice that an agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*; and

(c) commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.

Enforcing determinations

50.18 The *Privacy Act* contains provisions for the enforcement of determinations made under s 52. These mechanisms are different, depending on whether the respondent is an agency or organisation.

Enforcing determinations against organisations

50.19 The respondent to a determination under s 52 or an approved privacy code must not repeat or continue conduct covered by a declaration and must perform the act or course of conduct covered by the declaration.[25] These obligations are enforceable in the Federal Court or the Federal Magistrates Court in proceedings commenced by the complainant, the Commissioner, or an adjudicator for the approved privacy code under which the determination was made.[26] If satisfied that the respondent has engaged in conduct that constitutes an interference with the privacy of the complainant, the court 'may make such orders (including a declaration of right) as it thinks fit'.[27] The court is

25 *Privacy Act 1988* (Cth) s 55. Section 52 of the *Privacy Act* sets out the declarations the Privacy Commissioner can make in a determination.
26 Ibid s 55A(1).
27 Ibid s 55A(2).

to deal with the question of whether the respondent has engaged in conduct that constitutes an interference with privacy by way of a hearing de novo.[28]

Enforcement of determinations against agencies

50.20 As with organisations, an agency must not repeat or continue conduct covered by a declaration and must perform the act or course of conduct covered by the declaration.[29] Where the respondent to a determination is the principal executive of an agency, he or she is responsible for ensuring that the determination is brought to the attention of the relevant members, officers and employees of the agency and that those people desist from or perform conduct covered by the declaration.[30]

50.21 Unlike enforcement of determinations against organisations, where a determination against an agency or principal executive includes a declaration for compensation or reimbursement for expenses, the *Privacy Act* provides that the complainant is entitled to be paid the amount specified. The amount is recoverable either as a debt due to the complainant by the agency or the Commonwealth.[31] If an agency or the principal executive of an agency fails to comply with obligations arising from a declaration, the Commissioner or complainant can apply to the Federal Court or Federal Magistrates Court for an order directing the agency or principal executive to comply.[32] In contrast to the provisions for organisations, the court does not have to assess, by way of a hearing de novo, whether the agency engaged in conduct that constituted an interference with privacy. Rather, on application under the Act, the court may make 'such other orders as it thinks fit with a view to securing compliance by the respondent'.[33]

50.22 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* provisions for enforcing determinations are adequate and administered effectively.[34] The Australian Privacy Foundation described the enforcement provisions as 'unfortunate' in that complainants and the Commissioner have to go through a hearing de novo to enforce a determination if an agency or organisation fails to comply with its terms.[35]

---

28 Ibid s 55A(5).
29 Ibid s 58.
30 Ibid s 59.
31 Ibid s 60. This provision does not apply to organisations because of the limitations on Commonwealth judicial power: this issue is discussed further in Ch 3.
32 Ibid s 62.
33 Ibid s 62(4). See also s 61(5) regarding timing of the application.
34 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–17.
35 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

ALRC's view

50.23 In DP 72, the ALRC identified some concerns about the process of enforcing determinations in the Federal Court. Given the constitutional restrictions on the Commissioner exercising judicial power,[36] however, the ALRC does not recommend any amendments to the enforcement provisions. The ALRC notes, however, that its recommendation that the *Privacy Act* should be amended to provide for a complainant or respondent to seek merits review of determinations made by the Commissioner under s 52 may provide an alternative, and less costly, 'enforcement' mechanism for complainants than is currently provided in the Act.[37]

Reports by the Commissioner

50.24 The Commissioner has powers to report on the exercise of some of his or her functions. In addition to the reporting obligations following certain own motion investigations discussed above, where the Commissioner has monitored an activity or conducted an audit in the performance of the functions in ss 27, 28 and 28A of the *Privacy Act*, the Commissioner may report to the Minister about the activity or audit, and must report if directed to do so by the Minister.[38] The Commissioner can give a further report to the Minister where the Commissioner believes it is in the public interest to do so, and the Minister must lay such reports before each House of Parliament within 15 sitting days.[39]

50.25 There is no express power or obligation to report investigations of complaints and the *Privacy Act* does not envisage explicitly the Commissioner reporting directly to Parliament.[40] The ability to report on the results of audits, however, provides the Commissioner with another kind of 'enforcement' mechanism, as such reporting can involve a measure of publicity and sanction.

Injunctions

Background

50.26 The *Privacy Act* contains detailed provisions regarding the granting of injunctions. Section 98 provides that following an application from the Commissioner or another person, the Federal Court or Federal Magistrates Court can grant an injunction restraining a person from engaging in conduct that would constitute a

---

36 See the discussion in Ch 49.

37 See Rec 49–7. This was suggested by the Office of the NSW Privacy Commissioner: Privacy NSW, *Submission PR 193*, 15 February 2007.

38 *Privacy Act 1988* (Cth) s 32. The relevant Minister is currently the Cabinet Secretary. Certain matters may be excluded from reports—see *Privacy Act 1988* (Cth) s 33.

39 *Privacy Act 1988* (Cth) ss 30(4)–(5), 31(4)–(5), 32(2)–(3).

40 See Ibid s 30(6). See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.38]; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 128.

contravention of the *Privacy Act* and, if the court thinks it desirable to do so, requiring a person to do any act or thing.[41] An injunction may be granted if it appears to the court that it is likely the person will engage in the relevant conduct if the injunction is not granted, whether or not the person has previously engaged in conduct of that kind, and whether or not there is an imminent danger of substantial damage to any person if the person engages in the relevant conduct.[42] Where the Commissioner applies for an injunction under s 98, the court will not require the Commissioner or any other person to give an undertaking as to damages.[43]

50.27 Two features of the injunctions power are significant. First, it does not concern only enforcement of determinations.[44] It is a freestanding provision that deals with any contravention of the *Privacy Act*. Secondly, the 'standing' requirement is relatively easy to satisfy—the application may be made by the Commissioner 'or any other person'.[45]

50.28 There appear to be few cases in which an injunction has been granted to restrain contravention of the *Privacy Act*, though the remedy is potentially of general application and utility.[46] The OPC has stated that the Commissioner would seek an injunction only 'when other more informal means have failed to yield a satisfactory outcome'.[47]

Submissions and consultations

50.29 In DP 72, the ALRC noted comments by stakeholders on the injunctions power in the *Privacy Act*. While a number of stakeholders supported the power as it currently is expressed, including the standing requirements, the OPC expressed concern about the breadth of the standing provision. In particular, the OPC suggested that 'it could allow a party with no interest in the privacy of the individuals in question to seek an injunction that may, as a consequence, impact on how an agency or organisation interacts with that individual'.[48] The OPC recommended that s 98 be amended to include a more rigorous test for standing.

---

41 *Privacy Act 1988* (Cth) s 98(1)–(2).
42 Ibid s 98(5)(b). See also s 98(6).
43 Ibid s 98(7).
44 See N Witzleb, 'Federal Court Strengthens Privacy Enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 *Australian Business Law Review* 45, 45.
45 This is similar to the position in the *Trade Practices Act 1974* (Cth) s 80. See also *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* (2004) 148 FCR 145, [40], [55].
46 See *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* (2004) 148 FCR 145.
47 Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001), 3.
48 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

50.30 In contrast, another stakeholder described the ability of non-government organisations to seek injunctions because of the provision for open standing—as a 'theoretically valuable means by which contesting interpretations of principles could be resolved'.[49] In addition, the Australian Privacy Foundation submitted that the injunction power is valuable and that the Commissioner should make greater use of the power, 'both during complaint investigations and as a pro-active tool where interferences with privacy are brought to attention in other ways'.[50] The Queensland Council for Civil Liberties saw no reason to alter the position in relation to obtaining injunctions.[51]

50.31 In response to DP 72, the Cyberspace Law and Policy Centre submitted that:

> The Commissioner's ability to seek an injunction is potentially a particularly valuable aspect of the *Privacy Act* … because it carries with it the requirement that the Commissioner must also seek an interpretation of the Act by the Federal Court, rather than applying what the Commissioner's Office imagines is the law. Given that there are no useful decisions on the *Privacy Act* after 20 years—except one where one commercial party used the injunction provision against another—the opportunity for the Commissioner to seek judicial guidance on difficult aspects of the Act would be a rare and valuable opportunity, but it is one the Commissioner has never taken up.[52]

50.32 The Centre argued that greater use of the injunction power could be made if the OPC was given more resources to allow it to pursue injunctions and the *Privacy Act* was amended to allow non-government organisations or complainants to request the Commissioner to use the injunction power.[53]

ALRC's view

50.33 The ALRC does not recommend any reform to the injunctions provision. The power is comparable to provisions for statutory injunctions under the *Trade Practices Act 1974* (Cth) (TPA) and the *Corporations Act 2001* (Cth).[54] While the provisions have not been utilised often, the power itself is appropriate. The ALRC also recognises the value in providing for open standing in this area, because it allows consumer and privacy organisations to initiate proceedings under the section.[55] As noted by Dr Norman Witzleb:

> This may prove of particular use where large organisations introduce services which have the potential of presenting privacy threats on a massive scale—such as, for

---

49 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007. The ability to seek an injunction was said to be 'inherently valuable'.

50 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

51 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

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

53 Ibid.

54 See *Trade Practices Act 1974* (Cth) s 80; *Corporations Act 2001* (Cth) s 1324.

55 See also Australian Law Reform Commission, *Beyond the Door-keeper: Standing to Sue for Public Remedies,* ALRC 78 (1996).

example, the recently introduced 'g-mail' service by *Google*, which prompted substantial criticism from privacy and consumer groups worldwide.[56]

50.34 Greater use could be made of the injunctions power in the future, where, for example, new technologies raise such serious concerns that it is thought necessary to stop the conduct. The injunctions power may also come into play more if the ALRC's recommendation that the *Privacy Act* be amended to empower the Commissioner to direct an agency to prepare a privacy impact assessment is implemented.[57] If a project raised serious privacy concerns and the Commissioner believed it would, if implemented, interfere with the privacy of individuals, the Commissioner could seek an injunction from the Federal Court or Federal Magistrates Court to stop the project.[58]

Other enforcement mechanisms following non-compliance

Enforcement pyramid

50.35 As discussed in Chapter 4, Professors Ian Ayres and John Braithwaite have suggested that the ideal regulatory approach to enforcing compliance with regulation is through the adoption of an explicit 'enforcement pyramid'. Under such a model, regulators use coercive sanctions only when less interventionist measures have failed to produce compliance.[59] Breaches of increasing seriousness are dealt with by sanctions of increasing severity, with the most serious or 'ultimate sanctions' generally held in reserve as a threat.

50.36 There is great value in adopting the enforcement pyramid structure in the *Privacy Act*, as discussed further in Chapter 45. In some respects, the *Privacy Act* already adopts a pyramid-type structure for enforcing compliance. The approach relies initially on encouraging compliance, with determinations (and enforcement in the courts) and injunctions held in reserve. While there is some degree of escalation involved in these remedies, there are currently no civil penalties for serious contraventions of the Act, and only some limited criminal penalties attached to credit reporting, and tax file number, offences.[60]

---

56 N Witzleb, 'Federal Court Strengthens Privacy Enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 *Australian Business Law Review* 45, 49.

57 See Rec 47–4.

58 See *Privacy Act 1988* (Cth) s 98.

59 The model was first put forward in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985) and was further discussed in B Fisse and J Braithwaite, *Corporations, Crime and Accountability* (1993); C Dellit and B Fisse, 'Civil and Criminal Liability Under Australian Securities Regulation; The Possibility of Strategic Enforcement' in G Walker and B Fisse (eds), *Securities Regulation in Australia and New Zealand* (1994), 570.

60 The ALRC recommends the repeal of these credit reporting offences: see Rec 59–9.

Issues Paper 31

50.37 In IP 31, the ALRC asked whether the range of remedies available to enforce rights and obligations created by the *Privacy Act* required expansion. Further remedies suggested by the ALRC included administrative penalties, enforceable undertakings or other coercive orders, remedies in the nature of damages, infringement notices, civil penalties and criminal sanctions.[61]

50.38 The ALRC received mixed responses from stakeholders about the need for further enforcement mechanisms. Some stakeholders suggested that harsher penalties under the *Privacy Act* are unnecessary as it has not been shown that the lack of 'teeth' in privacy legislation has reduced compliance with privacy laws.[62] In contrast, the Australian Privacy Foundation submitted that a wider range of remedies and sanctions is desirable.[63]

50.39 A number of stakeholders in the OPC Review submitted that there should be some level of civil penalty resulting from a contravention of the *Privacy Act*.[64] One stakeholder stated that it is hard to convince some company boards to comply with privacy laws when no schedule of penalties is attached to non-compliance with the NPPs.[65] While recognising the resource implications of additional remedies, the Consumer Credit Legal Centre observed in a submission to the Inquiry that:

> stronger enforcement mechanisms, including through civil pecuniary penalties, present the OPC with a more long-term cost-effective way of functioning. Forcing businesses and industry to be accountable by imposing greater deterrents should result in less cases and investigations by the OPC.[66]

50.40 There was no support for introducing further criminal penalties into the *Privacy Act*, such as for a reckless, intentionally dishonest or flagrant contravention. The OPC considered that a cautious approach should be taken to the inclusion of further criminal sanctions, and noted that 'as privacy is unlikely to be a high policing priority, a significant increase in criminal sanctions may impede rather than facilitate better privacy protection and privacy complaint outcomes'.[67]

---

61 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–22. The remedies are discussed in more detail at [6.180]–[6.205].

62 See, for example, Australian Health Insurance Association, *Submission PR 161*, 31 January 2007.

63 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007. See also New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007.

64 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 132–133.

65 Ibid, 133. This view also was expressed in a number of the ALRC's consultations conducted during this Inquiry.

66 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160*, 31 January 2007.

67 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

Discussion Paper proposal

50.41 In DP 72, the ALRC canvassed whether the range of remedies available to enforce rights and obligations created by the *Privacy Act* required expansion. A number of suggestions were made by stakeholders, including enforceable undertakings, civil penalties and coercive orders. Having regard to the enforcement pyramid concept, the ALRC proposed 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.[68]

Submissions and consultations

50.42 The ALRC received a number of submissions on this proposal. The OPC expressed its support for allowing the imposition of a civil penalty in the case of serious or repeated interferences with privacy. It argued that the definition of 'serious' should include explicitly cases where a respondent breaches a notice to comply arising from an own motion investigation, or where a respondent fails to report a data breach, contrary to the requirements of the *Privacy Act*.[69]

50.43 The Law Council of Australia argued that a civil penalty was preferable to the introduction of administrative penalties[70] or an infringement notice scheme and was consistent with the 'light-touch' approach of the *Privacy Act*.[71] PIAC stated that a civil penalty regime was likely to provide a strong incentive to comply with the Act, provided that the amount of the penalty was commensurate with the seriousness of the breach.[72] A number of other stakeholders also supported this proposal.[73]

50.44 Some stakeholders also agreed with the proposal that the OPC should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty will be made.[74] The Law Council argued that:

---

68 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 46–2. See also Proposal 55–8, in relation to credit reporting.

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

70 Administrative penalties in Australian law are sanctions imposed by a regulator, or by a regulator's enforcement of legislation, without intervention by a court or tribunal.

71 Law Council of Australia, *Submission PR 527*, 21 December 2007.

72 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007

73 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Lawyers Alliance, *Submission PR 528*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

74 BUPA Australia Health, *Submission PR 455*, 7 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007. See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 46–2.

> A binding set of criteria would provide necessary certainty to the scheme and prevent organisations from incurring significant costs associated with determining what obligations exist.[75]

50.45 One stakeholder expressed the view that the *Privacy Act* should include criminal sanctions for serious irresponsible handling of personal information. It argued that criminal sanctions should apply to the senior management and directors of agencies and organisations.[76]

50.46 Other stakeholders took the view that the introduction of civil penalties was unnecessary.[77] GE Money, for example, submitted that it was not aware of 'the sorts of significant and ongoing breaches of privacy laws by organisations that might suggest that such a regime were necessary'.[78] Another stakeholder argued that:

> To the extent that there is a need to increase compliance with and enforcement of the Act, this can easily be met by using the existing powers of the Privacy Commissioner to a greater extent.[79]

ALRC's view

50.47 The framework of compliance-oriented regulation underpinning the *Privacy Act* should be considered when examining whether there should be further penalties added to the Act. As discussed in Chapter 45, a compliance-oriented approach to enforcement, which includes a focus on fostering compliance in the first instance, requires the presence of punitive sanctions to be effective. This is because 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.[80] The existence of a strong penalty, by itself, can act as an incentive for compliance, as long as the regulated entity knows that the regulator will impose the penalty where appropriate.

50.48 Determinations are regarded by some as a 'strong' penalty, because they can involve a public declaration of breach and thereby contain an element of informal, negative publicity.[81] The ALRC notes, however, that according to the OPC's determination policy, determinations are not necessarily going to be limited to the most serious cases, 'nor will determinations issued by the Commissioner necessarily be

---

75 Law Council of Australia, *Submission PR 527*, 21 December 2007.

76 Smartnet, *Submission PR 457*, 11 December 2007.

77 GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007.

78 GE Money Australia, *Submission PR 537*, 21 December 2007.

79 Confidential, *Submission PR 536*, 21 December 2007.

80 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 539. See also J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science.

81 Determinations are published, with the respondent's name, at Office of the Privacy Commissioner, *Complaint Case Notes, Summaries and Determinations* (2007) <www.privacy.gov.au/act/casenotes/index.html> at 15 May 2008.

punitive'.[82] This approach by the OPC is consistent with the ALRC's recommendation to increase the number of determinations issued, by giving complainants and respondents the right to require the Commissioner to issue a determination in certain circumstances.[83]

50.49 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.[84] The Guide provides that the inclusion of civil penalty provisions is most likely to be appropriate and effective where:

- criminal punishment is not merited (for example, offences involving harm to a person or a serious danger to public safety should always result in a criminal punishment);
- the penalty is sufficient to justify court proceedings; and
- there is corporate wrongdoing.[85]

50.50 The inclusion of civil penalties in the *Privacy Act* is appropriate and justifiable by reference to each of the circumstances outlined above.[86] Criminal sanctions would be disproportionate to the level of harm caused by a serious or repeated interference with an individual's privacy. Financial penalties are, however, likely to be effective against agencies and organisations by providing a strong incentive to comply with the Act.

50.51 Although the significance of determinations should not be underestimated, there is a need to strengthen the overall enforcement remedies available in the *Privacy Act*. Accordingly, the ALRC recommends that the 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.[87] The Privacy Commissioner should be empowered to bring proceedings for pecuniary penalties in the Federal Court, similar to the approach taken with the Australian Competition and Consumer Commission (ACCC) under the TPA.[88]

---

82 Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2, 2.

83 See Rec 48–5.

84 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), [7.2].

85 Ibid, [7.2].

86 The ALRC has also recommended that civil as well as criminal penalties be available under Part 13 of the *Telecommunications Act 1997* (Cth). See Rec 71–3.

87 See also Rec 59–9 which recommends the imposition of a civil penalty for breaches of the credit reporting provisions.

88 *Trade Practices Act 1974* (Cth) s 77.

50.52 Consistently with the ALRC's recommendation in *Principled Regulation* (ALRC 95), the ALRC recommends that the OPC develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty under the *Privacy Act* would be made.[89] Examples of a serious or repeated interference with the privacy of an individual could include where the matter involves: an apparent blatant disregard of the law; a history of previous contraventions of the law; significant public detriment or significant number of complaints.[90] Civil penalties may also be pursued where there is the potential for action to have a worthwhile educative or deterrent effect. The ALRC agrees with the OPC that a serious interference with privacy should include cases where a respondent breaches a notice to comply. Failure to notify the Commissioner of a data breach as required by the Act, also may attract a civil penalty.[91]

50.53 Provision should also be made to allow for the Privacy Commissioner to accept an enforceable undertaking. An enforceable undertaking is essentially a promise enforceable in court. A breach of the undertaking is not contempt of court but, once the court has ordered the person to comply, a breach of that order is contempt.[92] Undertakings under s 87B of the TPA were introduced as an enforcement tool in 1993. Research undertaken for the ACCC in 2001 showed that undertakings were frequently used instead of court action, and often encompassed assurances by the offender to undertake a comprehensive compliance program. Undertakings also were made as part of the settlement of court proceedings.[93] Under the TPA provisions, undertakings may be published on the ACCC's website. This approach both lends transparency to the process and serves an educative function.

50.54 Since 2005, the Australian Communications and Media Authority (ACMA) has accepted enforceable undertakings about matters concerning compliance with the *Telecommunications Act 1997* (Cth). ACMA may accept undertakings

> that a person will take specified action or refrain from taking specified action to comply with [the Act], or take action directed at avoiding contravention in the future.[94]

---

89 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 10–1.

90 These factors are similar to the enforcement priorities of the ACCC: see Australian Competition and Consumer Commissioner, *Section 87B of the Trade Practices Act: A Guideline on the Australian Competition and Consumer Commission's Use of Enforceable Undertakings* (1999), 2.

91 See Rec 51–1.

92 See, eg, *Australian Securities and Investments Commission Act 2001* (Cth) ss 93A, 93AA.

93 K Yeung *The Public Enforcement of Australian Competition Law* (2001), 19–20.

94 *Telecommunications Act 1997* (Cth) Part 31A. Australian Communications and Media Authority *Guidelines for the Use of Enforceable Undertakings—Telecommunications Obligations* (2006), 1.

50.55 In ALRC 95, it was noted that regulators viewed enforceable undertakings as a success in terms of achieving compliance following a breach.[95] The Privacy Commissioner should be empowered, therefore, to accept an undertaking that an agency or organisation will take specified action to ensure compliance with the *Privacy Act* or other enactment under which the Commissioner has a power or function.

Recommendation 50–2 The *Privacy Act* should be amended to allow the Privacy Commissioner to seek a civil penalty in the Federal Court or Federal Magistrates Court where there is a serious or repeated interference with the privacy of an individual.

Recommendation 50–3 The Office of the Privacy Commissioner should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty will be made.

Recommendation 50–4 The *Privacy Act* should be amended to empower the Privacy Commissioner to accept an undertaking that an agency or organisation will take specified action to ensure compliance with a requirement of the *Privacy Act* or other enactment under which the Commissioner has a power or function. Where an agency or organisation breaches such an undertaking, the Privacy Commissioner may apply to the Federal Court for an order directing the agency or organisation to comply, or any other order the court thinks appropriate.

95 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), 99.

51. Data Breach Notification

Contents

Introduction

51.1 Data breach notification is, in essence, a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information. It is a topical issue in privacy regulation around the world.

51.2 The Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) in the *Privacy Act 1988* (Cth) do not impose an obligation on agencies and organisations to notify individuals whose personal information has been compromised. The Act requires, however, that agencies and organisations take reasonable steps to maintain the security of the personal information they hold.[1]

1 *Privacy Act 1988* (Cth) s 14, IPP 4; sch 3, NPP 4. See also the recommended 'Data Security' principle in the Unified Privacy Principles set out at the beginning of this Report and in Ch 28.

51.3 This chapter begins by considering the rationales given for data breach notification laws in the United States (US), which is at the forefront in the development of such laws. The chapter then considers some of the key elements of data breach notification laws in other jurisdictions, including the event that triggers the requirement to notify. It also looks at the recent introduction in Australia and New Zealand of voluntary data breach notification schemes. Finally, the chapter sets out the ALRC's view on the justification for a data breach notification law and recommends that the *Privacy Act* be amended to include a new Part on data breach notification.

Rationale for data breach notification

Identity theft

51.4 In the US, concerns about identity theft and identity fraud have been the main issues driving the development of data breach notification laws.[2] As discussed in Chapter 12, identity theft is a subset of the broad concept of 'identity crime' and is used to describe the illicit assumption of a pre-existing identity of a living or deceased person, or of an artificial legal entity such as a corporation.[3] A stolen identity can be used to commit 'identity fraud', which is where a fabricated, manipulated or stolen identity is used to gain a benefit or avoid an obligation. An example of identity fraud is using a stolen identity to make fraudulent purchases or steal money from a victim (known as 'account takeover').[4] Another example of identity fraud is where a criminal uses personal information about an identity theft victim to open new accounts in the name of the victim (sometimes called 'true name fraud').[5]

51.5 With advances in technology, agencies and organisations are storing vast amounts of identifying information electronically.[6] Any breach of the secure storage of this information can result in the release of personal, identifying information of an individual. That personal information may be sufficient to allow an unauthorised person to assume the identity of the victim and use that illicit identity to open, for example, new accounts in the victim's name.

51.6 For these reasons, a security breach, resulting in unauthorised 'leaks' or acquisitions of information, is thought to contribute to the risk of identity theft, and the

---

2 See Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1. Ch 12 discusses identity theft—and the related concepts of 'identity crime' and 'identity fraud'—in more detail.

3 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.

4 See M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 2.

5 See Ibid, 2.

6 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1.

consequent risks of identity fraud.[7] By requiring notice to persons who may be affected adversely by a breach, data breach notification laws 'seek to provide such persons with a warning that their personal information has been compromised and an opportunity to take steps to protect themselves against the consequences of identity theft'.[8] As one commentator explains:

> Identity theft and identity fraud have emerged as serious crimes for consumers, citizens and business … Given the peculiar nature of this type of theft—namely, that it can be perpetrated by accessing information stored in places uncontrolled by the victim and in places of which the victim is often unaware—legislators have passed or are considering passing laws which require that the consumer be notified in the event of a data breach.[9]

51.7 Data breach notification laws are, therefore, based on the recognition that 'individuals need to know when their personal information has been put at risk in order to mitigate potential identity fraud damages'.[10]

Lack of market incentives for notification

51.8 Some commentators suggest that the obligation to notify individuals of a data breach needs to be mandated legally because the market, by itself, may not provide sufficient incentives for organisations to take measures to notify individuals affected by the breach.[11] In particular, an organisation may not have an incentive to notify individuals affected by a security breach when the cost of the notification exceeds the expected damage to the organisation.[12]

51.9 The cost of notification does not just include the actual cost involved in notifying every individual affected by a security breach, although that, by itself, can be very expensive. Notifying customers of a security breach also gives rise to a real potential for market damage to the organisation, including reputational damage, lost customers and lost future profits. Notification also can expose an organisation to civil penalties from regulators and costly private litigation proceedings by individuals

---

7 See M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

8 T Smedinghoff, *Security Breach Notification—Adapting to the Regulatory Framework* (2005) Baker & McKenzie <www.bakernet.com/ecommerce> at 31 July 2007, 1–2. See also M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 11; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1–2.

9 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 2.

10 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 2.

11 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 11–12.

12 Ibid, 12.

affected. If the organisation has a high profile or the security breach is large, notification also can result in negative publicity in the media. In these circumstances, an organisation may avoid reporting a security breach if it is not legally required to do so, as the cost to the organisation of notifying individuals significantly outweighs the costs caused by the actual breach. For these reasons, it has been observed that, in the absence of a legal requirement to notify, market forces may 'undersupply notification'.[13]

Incentives to secure data

51.10 Given the reputational damage that can flow from having to disclose a security breach, it has been suggested that the existence of a data breach notification law provides commercial incentives for organisations to take adequate steps in the first place to secure data.[14] The purpose of the Delaware data breach notification legislation, for example, is to 'help ensure that personal information about Delaware residents is protected by encouraging data brokers to provide reasonable security for personal information'.[15] This is an important effect of data breach notification, particularly as organisations in the US may not be subject to data security obligations such as those in the *Privacy Act*.[16]

Increasing number of data breaches

51.11 The rapid growth in data breach notification laws in the US in the past few years is said to be a direct response to a series of high profile, well-publicised data breaches.[17] One of the most notorious data breaches was the disclosure by ChoicePoint, a large identification and credential verification organisation, of sensitive information it had collected on 145,000 individuals.

51.12 The Privacy Rights Clearinghouse maintains a Chronology of Data Breaches, which lists all breaches reported in the US that expose individuals to identity theft or breaches that qualify for disclosure under state laws. As at 28 April 2008, the total number of records containing sensitive personal information involved in security breaches was 226 million.[18] It also is important to note that not all data breach incidents have involved electronic records. For example, in Florida, the medical records of 27 hospital patients were discovered being used as scrap paper in a Utah

---

13 Ibid, 13.

14 B Arnold, 'Losing It: Corporate Reporting on Data Theft' (2007) 3 *Privacy Law Bulletin* 101, 102. See also T Smedinghoff, *The New Law of Information Security: What Companies Need to Do Now* (2005) Baker & McKenzie <www.bakernet.com/ecommerce> at 31 July 2007; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 22.

15 *Delaware Code* , Synopsis. Similar comments are made in *Arkansas Code* § 4-110-102.

16 Some of the data breach notification laws, however, also require regulated entities to implement and maintain reasonable security procedures and practices: see, eg, *Arkansas Code* § 4-110-104.

17 See Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1–2. See also T Smedinghoff, *Security Breach Notification—Adapting to the Regulatory Framework* (2005) Baker & McKenzie <www.bakernet.com/ecommerce> at 31 July 2007, 1.

18 Privacy Rights Clearinghouse, *A Chronology of Data Breaches—Updated to 28 April 2008* <www.privacyrights.org/ar/ChronDataBreaches.htm> at 29 April 2008.

primary school classroom.[19] Security breaches, therefore, are a concern in the US community.

51.13 There also have been high profile data breaches in the United Kingdom (UK). In 2007, the UK Government's HM Revenue and Customs department, which is responsible for collecting tax revenue as well as paying tax credits and child benefits, lost two CDs containing confidential information—including the dates of birth, addresses, bank accounts and national insurance numbers—of over 25 million child benefit recipients. The entire child benefit database was sent by a junior official from a regional office to the National Audit Office in London via courier and without a registration or a tracking number.[20] Following the breach, the UK Government made a commitment to amend the *Data Protection Act 1998* (UK) to allow the Information Commissioner to carry out inspections of organisations that collect and use personal information and provide new sanctions for breaches of the data protection principles.[21]

Models of data breach notification laws

51.14 There are a number of proposed or established models for data breach notification laws. California was the first US state to require the reporting of data breaches involving personal information. The Californian law has been a model for legislation passed in over 30 US state legislatures and there are moves to implement a national notification standard concerning compromised data.[22] While many US states adopt very similar provisions to the Californian law, some set a different test of when notification will be required.

51.15 While organisations are subject to differing data breach notification requirements, depending on their state of operation, all financial institutions in the US are subject to the data breach notification requirements set out in the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, issued by the US Department of Treasury and other agencies (US Interagency Guidance). The US Interagency Guidance interprets the requirements of the *Gramm-Leach-Bliley Act of 1999* (US), which regulates all financial services institutions in the US, to develop and implement a response program 'to address unauthorized access to, or use of customer information that could result in substantial

---

19 A Falk 'Health Files are Sold as Scrap Paper to Utah' *Deseret Morning News* (online), 10 March 2008, <www.deseretnews.com/article/1,5143,695260327,00.html>. The need for security and destruction requirements to extend to hard copies of documents is discussed in Ch 28.

20 P Wintour, 'Lost in the Post—25 Million at Risk after Data Discs go Missing', *The Guardian* (online) 21 November 2007, <www.guardian.co.uk>.

21 United Kingdom Information Commissioner's Office, 'Information Commissioner Welcomes Government's Commitment to Strengthen the Powers of the ICO' (Press Release, 17 December 2007).

22 M Coyle, 'Industry, Government Fret Over Tactics for Fighting Data Theft', *National Law Journal* (online), 10 August 2006, <www.law.com/jlp/nlj/index.jsp>.

harm or inconvenience to a customer'.[23] The US Interagency Guidance only applies to financial services institutions, and does not apply to other organisations or federal or state government agencies.

51.16 In Canada, only the province of Ontario requires notification after a security breach.[24] There also have been moves at the federal level in Canada to introduce a data breach notification law. The Canadian Internet Policy and Public Interest Clinic (CIPPIC) issued, in January 2007, a White Paper, *Approaches to Security Breach Notification*, which puts forward a model law for Canada. In addition, the review of the *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act), by the Canadian Government Standing Committee on Access to Information, Privacy and Ethics, considered the issue of breach notification. The Committee recommended that the PIPED Act be amended to include a breach notification provision requiring organisations to report certain defined breaches of personal information holdings to the Canadian Privacy Commissioner. The Canadian Privacy Commissioner would then determine whether affected individuals and others should be notified and, if so, in what manner.[25]

51.17 In 2007, Australian Democrats Senator Natasha Stott-Despoja put forward a Private Members Bill amending the *Privacy Act* to require agencies and organisations to report data breaches where there has been a confirmed or reasonably suspected breach of data security—defined to mean the unauthorised acquisition, transmission, disclosure or use of personal information involving an unauthorised party. Notification would be required as soon as possible after the breach,[26] and must include a description of the breach, the action taken by the agency or organisation to recover the information and measures taken to prevent a re-occurrence of the breach. The Bill also required the agency or organisation to maintain a register of notifications made and the action taken to comply with the obligations under the Bill.[27]

51.18 In April 2008, the Office of the Privacy Commissioner (OPC) released a consultation paper seeking stakeholder views on a draft Voluntary Information Security Breach Notification Guide developed to assist agencies and organisations to 'respond effectively to an information security breach'.[28] The OPC noted the ALRC's proposal in the Discussion Paper, *Review of Australian Privacy Law* (DP 72), to amend

---

23 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). See *Gramm-Leach-Bliley Act 1999* 15 USC §§ 6801–6809 (US).

24 See *Personal Health Information Protection Act 2004* (Ontario) s 12.

25 Canadian Government Standing Committee on Access to Information Privacy and Ethics, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)—Fourth Report* (2007), 45.

26 Privacy (Data Security Breach Notification) Amendment Bill 2007 (Cth) sch l, cls 1 and 2.

27 Ibid sch 1, cl 2. As at 20 May 2008, the Bill had been read for a second time in the Senate.

28 Australian Government Office of the Federal Privacy Commissioner *Consultation Paper—Draft Voluntary Information Security Breach Notification Guide* (2008), 4.

the *Privacy Act* to include a data breach notification provision. It stated that the voluntary guidelines are not intended to be a substitute for further legislative action, but are aimed at encouraging voluntary action to address these issues while legislative change is under consideration. The draft Guide suggests that agencies should consider notification where the security breach creates a real risk of serious harm to the individual. A notice should include: a description of the incident; the response of the agency or organisation to the breach; what assistance will be offered by the agency or organisation to the individual; whether the OPC has been notified; and how a complaint can be lodged with the OPC.[29]

51.19 The OPC voluntary guidelines are based on similar guidelines issued in 2007 by the Privacy Commissioners of Canada and New Zealand.[30] The Privacy Commissioners of British Columbia and Ontario also have issued a 'Breach Notification Assessment Tool' to assist organisations in determining what steps should be taken in the event of a privacy breach. The New Zealand Privacy Commissioner has indicated that amendments to the *Privacy Act 1993* (NZ) to introduce mandatory breach notification should be considered in the future.[31]

51.20 While there is a similarity of purpose to the above laws, they adopt a variety of approaches on key areas such as the triggering event, exceptions to the notification requirement and responsibility to notify. The following section focuses on the key approaches taken in data breach notification laws in California and other US states, the US Interagency Guidance and the CIPPIC proposal in Canada.

Trigger for notification

51.21 In California, the event that triggers the obligation to provide notice is any 'breach of the security of the system', which is defined as the 'unauthorised acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency'.[32] A good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency does not constitute a breach of the security of the system, 'provided that the personal information is not used or subject to further unauthorised disclosure'.[33] This is said to

29 Ibid, 27–29.

30 See Office of Privacy Commissioner of Canada, *Key Steps for Agencies in Responding to Privacy Breaches* (2007) and New Zealand Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (2007).

31 New Zealand Privacy Commissioner 'Draft Privacy Guidelines Announced', (Press Release, 27 August 2007). The New Zealand Law Commission also is currently undertaking a reference on privacy, including review and update of the *Privacy Act 1993* (NZ): see Ch 1.

32 *California Civil Code* § 1798.29(a).

33 Ibid § 1798.29(d).

provide an exception to the general obligation to notify for 'harmless internal breaches'.[34]

51.22 The Californian triggering event of any 'unauthorised acquisition' of computerised data sets quite a low threshold for notification. It requires notification even if the organisation considers it very unlikely that the personal information acquired could give rise to a risk of harm or identity theft. While this triggering event has been followed in a number of other US states,[35] some have adopted a higher threshold for notification. For example, the *Indiana Code* requires notification where there has been unauthorised acquisition of personal information 'if the database owner knows, should know, or should have known that the unauthorised acquisition constituting the breach has resulted in or could result in identity deception, identity theft or fraud affecting the Indiana resident'.[36] Other US states provide an exception to notification if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.[37]

51.23 In its approach to defining the triggering event, the US Interagency Guidance gives the relevant organisation greater discretion to decide whether notification is necessary. The US Interagency Guidance provides that when an institution becomes aware of an incident of unauthorised access to sensitive customer information, the institution should conduct a reasonable investigation to determine promptly the likelihood that the information has been, or will be, misused. If the institution determines that misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible.[38]

51.24 In its proposed model for Canada, the CIPPIC picked up on the Californian triggering event of 'acquisition or reasonable belief of acquisition by an unauthorised person'. The CIPPIC argued that this standard 'is higher than mere "access by an unauthorised person", but lower than standards that incorporate a "risk of identity fraud" element'.[39] The CIPPIC suggested that:

> The test should be designed to avoid notification obligations where the breach does not expose individuals to a real risk of identity theft, but to apply in all situations where such a risk is created.[40]

---

34 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

35 See, eg, *Delaware Code* §§ 12B-101–12B-102; *New York State Code* § 899-aa(1).

36 *Indiana Code* § 24-4.9-3-1(1)(a). A similar approach is taken in *Ohio Revised Code* § 1347.12(B)(1).

37 See, eg, *Arkansas Code* § 4-110-105(d).

38 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).

39 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 24.

40 Ibid, 25.

Definition of 'personal information' in data breach notification laws

51.25 The data breach notification laws in each state define the type of personal information that, when leaked, may give rise to the obligation to notify. For the purpose of data breach notification, the definition of 'personal information' tends to focus more on the combination of certain pieces of personal information rather than providing a broad definition like that provided in the *Privacy Act*. References to 'personal information' in the context of data breach notification, therefore, are not meant to refer to personal information as defined in the *Privacy Act*.

51.26 The general approach adopted in a number of states, including California, is to define personal information as an individual's first name (or initial) and last name, in combination with any of the following:

- social security number;
- driver's licence number or state identification card number; or
- account number, credit card number or debit card number in combination with any necessary security code, access code or password that would permit access to the account.[41]

51.27 Some US states include medical information in the definition of 'personal information'. For example, the Delaware code defines 'personal information' as including 'individually identifiable information, in electronic or physical form, regarding the Delaware resident's medical history or medical treatment or diagnosis by a health care professional'.[42]

51.28 The CIPPIC's proposed law for Canada defines 'designated personal information' in a similar manner as California, although it includes the combination of an address by itself (that is, without a name as well), with other sensitive information within the definition of 'designated personal information'. The CIPPIC justified this approach on the basis that 'it is relatively easy to obtain a person's name from an address, using phone books, online databases and search engines'.[43]

---

41 *California Civil Code* § 1798.29(e). A similar definition is adopted in 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).

42 *Delaware Code* § 12B-101(2). See also *Arkansas Code* § 4-110-103.

43 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

51.29 Under the Californian definition and that of a number of other US states, personal information does not include 'publicly available information that is lawfully made available to the general public from federal, state, or local government records'.[44] The US Interagency Guidance, however, outlines that it would be inappropriate to exclude publicly available information from the definition of sensitive customer information, where the publicly available information is otherwise covered by the definition of customer information. For example, while a personal identifier, such as a name or address, may be publicly available, it is sensitive customer information when linked with particular non-public information such as a credit card account number.[45]

Exceptions

Encryption

51.30 Most states that have data breach notification laws, including California, do not require notification where the personal information that was the subject of the unauthorised acquisition was encrypted.[46] Some US states specify that the exception does not apply where the encryption key also was acquired.[47] The CIPPIC model also made an exception for encrypted data.[48]

51.31 In contrast, the US Interagency Guidance rejected a blanket exclusion for encrypted data because 'there are many levels of encryption, some of which do not effectively protect customer information'.[49]

51.32 To address the differing standards of encryption and provide more guidance to organisations, some US states define encryption in the relevant statute. For example, the *Indiana Code* provides that data are encrypted for the purposes of the data breach notification law if data:

> (1) have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or
>
> (2) are secured by another method that renders the data unreadable or unusable.[50]

---

44 *California Civil Code* § 1798.29(f). See also *New York State Code* § 899-44(1)(b); *Delaware Code* §§ 12B-101(2); *Ohio Revised Code* § 1347.12(A)(6).

45 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).

46 *California Civil Code* § 1798.29(a).

47 See, eg, *New York State Code* § 899-44(1)(b); *Indiana Code* § 24-4.9-3-1(1)(a)(2).

48 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

49 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).

50 *Indiana Code* § 24-4.9-2-5. See also *Ohio Revised Code* § 1347.12(A)(4).

51.33 Others US states give the organisation discretion to determine what constitutes valid encryption under the statute.[51] As the CIPPIC explains, this 'provides latitude to organisations in selecting encryption applications that suit them'.[52]

Redaction

51.34 Some US states also provide an exception to notification for data that are redacted. Redaction can refer to a variety of practices. In Indiana, redaction is defined as data that are altered or truncated so that not more than the last four digits of a driver's licence number, stated identification number, or account number, are accessible as part of personal information.[53] The CIPPIC proposal for a Canadian data breach notification law also proposes exceptions for 'information that is redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable by unauthorized persons'.[54]

Responsibility to notify

51.35 In all US states and in the US Interagency Guidance, the responsibility for deciding whether notification is required following a breach in the security of the system rests with the organisation itself.[55] The CIPPIC adopted a similar approach in its proposed model for Canada, providing that organisations should have the responsibility for determining whether the standard for breach notification is met.[56] The CIPPIC acknowledged that generally the affected organisation is in the best position to calculate the associated risks of a breach of its information security and should be entrusted with this determination.[57]

---

51 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 14. For example, California does not define encryption in the Civil Code. It has, however, issued guidelines recommending that data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.

52 Ibid, 14.

53 *Indiana Code* § 24-4.9-2-11. See also *Ohio Revised Code* § 1347.12(A)(9).

54 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

55 See, eg, *California Civil Code* § 1798.29(a); *Ohio Revised Code* § 1347.12(B)(1); *Delaware Code* § 12B-102(a); *Indiana Code* § 24-4.9-3-1; *New York State Code* § 899-44(2); *Arkansas Code* § 4-110-105. See also 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).

56 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

57 Ibid, 26.

51.36 In all the proposed models considered by the ALRC, notification of the security breach was required to any individual affected by the breach.[58] In addition to notifying individuals affected, some US states require that the organisation notify the relevant consumer protection agency.[59] The US Interagency Guidance provides that an institution should notify its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorised access to, or use of, 'sensitive personal information'.[60] Similarly, the CIPPIC recommended in its proposed model for Canada, that

> there should be a requirement that every breach involving defined personal information be reported to the Privacy Commissioner, with full information about the nature and extent, the anticipated risks, mitigation measures, steps taken to notify affected individuals or, where notification is not considered warranted, the justification for not taking this step.[61]

51.37 Under the CIPPIC model, notice should be made to the Privacy Commissioner regardless of whether the test of individual notification is met. This would ensure that a record is kept of all security breaches, which provides oversight of organisational practices and 'offers the potential for organisations to obtain guidance from the Privacy Commissioner regarding notification obligations and methods'.[62] The CIPPIC also proposed that government agencies, credit bureaus and law enforcement authorities should be notified. The CIPPIC envisaged that the Privacy Commissioner would provide guidance to organisations as to which agencies should be notified in the context of a specific breach.[63]

Timing, method and content of notification

Timing of notification

51.38 In California, and most other US states with data breach notification laws, notification must occur in 'the most expedient manner possible and without unreasonable delay'.[64] The US Interagency Guidance provides that an institution must notify an affected customer 'as soon as possible' after concluding that misuse of the customer's information has occurred or is reasonably possible. Most US states, and the US Interagency Guidance, allow for delays in, or exceptions to, notification if notice will jeopardise a law enforcement investigation.

---

58 See, eg, *California Civil Code* § 1798.29(a); *Ohio Revised Code* § 1347.12(B)(1); *Delaware Code* § 12B-102(a); *Indiana Code* § 24-4.9-3-1; *New York State Code* § 899-44(2); *Arkansas Code* § 4-110-105. See also 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).

59 See, eg, *Delaware Code* § 12B-102(d).

60 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).

61 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 26.

62 Ibid, 26.

63 Ibid, 26–27.

64 *California Civil Code* § 1798.29(a).

51.39 The CIPPIC proposal for Canada adopted a similar approach. It proposed that notification should be undertaken 'as soon as possible and without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has made a written request for a delay'.[65]

Method of notification

51.40 The general approach of US state data breach notification laws is to describe the method of notification. For example, the *California Civil Code* provides that notice may be provided by written notice and electronic notice.[66] Other US states also allow notice by telephone or facsimile.[67]

51.41 California also provides for substituted notice where: the organisation demonstrates that the cost of providing notice would exceed $250,000; affected class of subject persons to be notified exceeds 500,000; or the agency does not have sufficient contact information. Substituted notice consists of: email notice, where the organisation has an email address for the subject persons; conspicuous posting of the notice on the organisation's website page, if the organisation maintains a website; and notification to major statewide media.[68]

51.42 Most US states have developed similar substituted notice schemes to handle large security breaches.[69] While the threshold and methods for substituted notice vary among states, a number of US states have adopted the same requirements as California.[70] In contrast to these approaches, the US Interagency Guidance prescribes a more general requirement that notice should be delivered 'in any manner that is designed to ensure that a customer can reasonably be expected to receive it'.[71]

51.43 In the CIPPIC's proposed model, notification 'should generally be by regular mail, but electronic and substitute notice should be permitted when certain conditions are met'.[72] In particular, email notice should be allowed only where the individual concerned has consented explicitly to receiving 'important notices such as this by email'. Substituted notice should be permitted where 'large numbers of individuals (eg, over 100,000) must be notified, where the total cost of individual notification is

---

65 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 28.

66 *California Civil Code* § 1798.29(g).

67 See, eg, *New York State Code* § 899-aa(5)(c); *Indiana Code* § 24-4.9-3-4(a).

68 See, eg, *California Civil Code* § 1798.29(g)(3).

69 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 17.

70 See, eg, *Arkansas Code* § 4-110-105(2); *Ohio Revised Code* § 1347.12(E).

71 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), 46.

72 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 28.

extraordinary (eg, over $150,000), or where the Privacy Commissioner has specifically approved the substitute notice'.[73] The CIPPIC proposed similar substituted mechanisms as provided in the Californian data breach notification law.

Form and content of notification

51.44 California does not specify the contents of the actual data breach notice. In contrast, other US states and the US Interagency Guidance provide detail on what should be covered in a notice. The general approach is to require the following information:

- a general description of what occurred, including the time and date of the breach and when it was discovered;
- the type of personal information that was the subject of the unauthorised access, use or disclosure;
- contact information for affected individuals to obtain more information and assistance; and
- a reminder of the need to remain vigilant and to report promptly incidents of suspected identity theft to the organisation.[74]

51.45 In its proposal for a Canadian data breach notification law, the CIPPIC proposed that breach notices include similar matters as set out above. It also suggested that the notice

> should be separate from other communications and should include detailed information about the breach, including an assessment of the risk that the personal information of affected individuals will be used in an unauthorized manner.[75]

Penalties for failure to notify

51.46 Some US states provide penalties for failure to make a disclosure or notification in accordance with the applicable law. For example, the *Indiana Code* provides that any person that fails to comply with the data breach notification law 'commits a deceptive act that is actionable only by the Attorney General'.[76] The Attorney General

---

73 Ibid, 28.

74 See, eg, *New York State Code* § 899-aa(5)(c). Similar matters are included in 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); Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

75 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 27.

76 *Indiana Code* § 24–4.9–4–1.

may bring an action to obtain an injunction or a civil penalty of not more than $150,000 per deceptive act.[77]

Discussion Paper proposal

51.47 In DP 72, the ALRC identified support in submissions and consultations for a requirement that data users notify individuals of a breach of their personal information in certain circumstances.[78] Supporters of a data breach notification law gave a number of reasons why such a law would be valuable. These include that it would:

- provide a strong market incentive and stimulus to organisations to secure databases adequately to avoid the brand and reputational damage arising from negative publicity;[79]
- encourage attention to compliance and vigilance against identity theft;[80] and
- improve accountability, openness and transparency in the handling of personal information by agencies and organisations.[81]

51.48 As set out in DP 72, support was not unanimous among stakeholders, and there were some organisations that did not support a mandatory data breach notification requirement. The trigger for notification was highlighted as the critical issue, with strong support expressed for the idea of making the reporting requirement proportionate to the potential for harm caused by the breach.

---

77 Ibid § 24–4.9–4–2. See also *Arkansas Code* § 4–110–108.

78 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Privacy NSW, *Submission PR 193,* 15 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 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; AAMI, *Submission PR 147,* 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; Microsoft Australia, *Submission PR 113,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Civil Liberties Australia, *Submission PR 98,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

79 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.

80 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Privacy NSW, *Submission PR 193,* 15 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

81 Privacy NSW, *Submission PR 193,* 15 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Health and Medical Research Council, *Submission PR114,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

51.49 After having regard to several factors, including the 'data abuse pyramid' postulated by Professor Daniel Solove,[82] the ALRC proposed that the *Privacy Act* be amended to include a new Part on data breach notification. The trigger for the requirement proposed by the ALRC was where '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'. Exceptions were provided, for example, where: the specified information was encrypted adequately; it was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the model Unified Privacy Principles (UPPs); or the Commissioner does not consider that notification would be in the public interest. Civil penalties were proposed for failure to notify the Commissioner of a data breach as required by the Act.[83]

Submissions and consultations

General

51.50 There continued to be strong support among stakeholders for the introduction of a requirement that data users notify individuals of a breach to their personal information where that breach may give rise to real harm to an individual.[84]

51.51 In particular, the OPC expressed strong support for the proposal. In its view, the more prescriptive and technology-specific approach taken in California is not appropriate to apply to the *Privacy Act*. The OPC also supported limiting the requirement to notify to circumstances where a breach is assessed as giving rise to a real potential for serious harm to an individual—on the basis that this higher threshold test would reduce the compliance burden on agencies and organisations. It agreed that the Privacy Commissioner should have the power to require notification where he or

---

82 Solove suggests that it is important for the law to intervene early to address cases of data insecurity, rather than only providing criminal sanctions for cases of identity fraud: see Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [47.55–47.62].

83 Ibid, Proposal 47–1.

84 Unisys, *Submission PR 569*, 12 February 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 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; Australia Post, *Submission PR 445*, 10 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; S Hawkins, *Submission PR 382*, 6 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007.

she believes that the unauthorised acquisition gives rise to a real risk of serious harm to any affected individual, even if the agency or organisation disagrees.[85]

51.52 A number of other stakeholders opposed the proposal. Telstra took the view that the proposed data breach notification requirement 'fails to achieve the right balance between the competing policy interests in this area'.[86] The Australian Direct Marketing Association (ADMA) was concerned that the operation of this proposal, in conjunction with the introduction of a statutory cause of action for serious invasion of privacy,[87] could result in an organisation incriminating itself by making a data breach notification which could then be used as evidence of an invasion of privacy.[88]

51.53 Some stakeholders stated that there was no need for a data breach notification requirement. The Australian Bankers' Association (ABA) noted that there is an express obligation under the *Privacy Act* to have in place adequate data security measures. It argued that this obligation, combined with the ALRC's proposed new enforcement powers for the Privacy Commissioner,[89] will ensure that there are sufficient 'commercial incentives' for organisations to secure data, without a need for breach notification requirements.[90]

51.54 Other organisations did not support the introduction of mandatory notification of serious data security breaches on the basis that it would impose too great a burden on business.[91] The Australian Information Industry Association submitted that:

> Coupled with the introduction of a statutory cause of action for invasion of privacy, a further additional burden on businesses is being suggested by the ALRC in the form of requiring notification of breach. Examples exist in overseas jurisdictions, such as the United States, where the requirements for notification make it difficult for any business to comply ...[92]

---

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

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

87 See Ch 74.

88 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007. This view was supported by Acxiom Australia, *Submission PR 551*, 1 January 2008.

89 See Ch 50.

90 See Ch 28.

91 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; BPay, *Submission PR 566*, 31 January 2008; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007. In relation to agencies, this view was shared by the Victoria Police: Victoria Police, *Submission PR 523*, 21 December 2007.

92 Australian Information Industry Association, *Submission PR 410*, 7 December 2007. This view was shared by IBM Australia, *Submission PR 405*, 7 December 2007.

51.55 Optus argued that businesses already deal with the issue of data breaches adequately. In its view:

> there is little recognition by the ALRC that organisations have been facing the risk of data security breaches for many years and that this risk, along with the many other risks, is constantly being managed by Australian businesses. There currently exists an environment where businesses know that a security breach could significantly undermine an organisation's or agency's reputation. Further, organisations are currently assessing risks to the individual created by a data security breach and deciding to contact affected parties.[93]

51.56 Google Australia argued that voluntary guidelines were a better approach to the issue than mandatory notification requirements. In Google's view:

> the real risk arising from the implementation of data breach legislation is to trivialise notification obligations in the mind of consumers to such an extent that they become meaningless and ineffective in terms of real data protection. In fact, the potential damage to consumers of a blanket notification obligation could be twofold: on the one hand, it can create unjustified anxieties and on the other hand, it may result in a lack of proper attention to more serious incidents (for example, if consumers come to regard numerous 'less serious' data breach notification emails as a form of spam).[94]

Triggers for notification

51.57 A number of stakeholders supported the data breach notification proposal in principle, but sought greater clarity as to when the notification requirements would be triggered. For example, a large number of stakeholders expressed the view that guidance from the OPC on what would constitute 'a real risk of serious harm' would be required.[95] The ABA argued that any evaluation of a 'real risk' should be done in consultation with stakeholders, and that assessments of risk should be industry specific.[96]

51.58 The Cyberspace Law and Policy Centre suggested that, if the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual, then there is no reason to limit the requirement to notify to specified classes of information.

---

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

94 Google Australia, *Submission PR 539*, 21 December 2007. The ABA also submitted that voluntary protocols would be a better alternative approach than mandatory notification requirements: Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

95 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Veda Advantage, *Submission PR 498*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Chartered Secretaries Australia, *Submission PR 351*, 28 November 2007. AXA noted that the introduction of a 'materiality' test (ie, where the material has an adverse effect on investors' interests) for reporting under the *Superannuation Industry (Supervision) Act 1993* (Cth) had been important: AXA, *Submission PR 442*, 10 December 2007.

96 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

In its view, 'the likelihood of serious harm should be a sufficient trigger in itself'.[97] In contrast, Microsoft Asia Pacific (Microsoft) argued that any data breach notification obligation should apply only in respect of unencrypted sensitive financial information, as it is most likely to be access to this type of information that leads to identity fraud.[98]

51.59 Some stakeholders felt that the ALRC had not set the bar for notification high enough, arguing that it should be required only where the unauthorised acquisition is 'likely' to result in a real risk of serious harm to any affected individual, rather than where it 'may give rise' to a real risk.[99] ADMA was concerned that the proposal would result in production of so many data breach notifications 'as to be both onerous for organisations and meaningless for consumers'.[100] The Insurance Council of Australia argued that only systemic breaches, as opposed to individual breaches, should be required to be reported.[101]

51.60 One stakeholder expressed the view that organisations will not always be in the position to know when information might be acquired by an 'unauthorised person' or if a particular person is in fact unauthorised.[102]

Role of the OPC

51.61 Some stakeholders questioned the proposed oversight role of the Privacy Commissioner.[103] Microsoft argued that the Commissioner's role in the data breach notification context should be confined to assessing whether any of the exceptions to notification apply, and not in deciding if notification is necessary.[104]

51.62 One stakeholder argued:

> The test should be whether an organisation or agency considers there to be such a risk. Otherwise, the test will have the effect of imposing a de facto obligation on organisations and agencies to notify the Privacy Commissioner of every data breach, however trivial. This is likely to impose significant and unnecessary costs on the organisations and agencies concerned and on the Privacy Commissioner. It is likely to take up Privacy Commissioner resources which could better be used for other purposes, such as education and complaint handling.[105]

---

97 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. This view was shared by Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

98 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

99 BPay, *Submission PR 566*, 31 January 2008; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

100 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007. This view was supported by Acxiom Australia, *Submission PR 551*, 1 January 2008.

101 Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

102 Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007.

103 For example, Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.

104 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

105 Confidential, *Submission PR 536*, 21 December 2007.

Exceptions to notification

51.63 The Department of Defence submitted that examples should be given of when notification would not be in the public interest. It recommended that these examples include breaches of information relating to national security.[106] The Australian Federal Police (AFP) also submitted that further consideration needed to be given to defining situations where the risk of notifying individuals would outweigh the benefits. In the AFP's view, this could include where an agency's internal processes have dealt appropriately with the person or system responsible for the disclosure and the individual to which the personal information relates has not been affected by that disclosure.[107]

51.64 Microsoft was of the view that adequate encryption should be considered an example of a circumstance where there is no real risk of serious harm to affected individuals, rather than as an exception to the notification obligation.[108] The Cyberspace Law and Policy Centre agreed that the operation of the exceptions needed to be clarified.[109]

51.65 The Cyberspace Law and Policy Centre also submitted that the Privacy Commissioner's power to determine that notification would not be in the public interest should be limited to substituting his or her view for that of the agency or organisation, or deferring notification until an investigation can be carried out.[110]

51.66 The Right to Know Coalition argued that there should be an exception for information supplied to a media organisation in circumstances which would be akin to a situation of qualified privilege under defamation law, or where the supply of the information was in the public interest.[111]

Form and content of notifications

51.67 The Law Council of Australia did not agree that organisations and agencies should include in a notice an assessment of the risk of identity fraud and the steps individuals can take to mitigate that risk. In its view, most organisations and agencies would be unqualified to advise on such matters and, therefore, the advice would not necessarily benefit individuals. It argued that the most appropriate entity to advise on steps to avoid identity fraud would be the OPC, which could publish guidelines on a website.[112] The Australian Unity Group agreed that such a requirement implies both an

---

106 Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.
107 Australian Federal Police, *Submission PR 545*, 24 December 2007.
108 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007. This view was shared by other stakeholders: see, eg, Confidential, *Submission PR 536*, 21 December 2007.
109 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
110 Ibid.
111 Right to Know Coalition, *Submission PR 542*, 21 December 2007.
112 Law Council of Australia, *Submission PR 527*, 21 December 2007. This view was shared by another stakeholder: Confidential, *Submission PR 536*, 21 December 2007.

element of expertise by an organisation in the area of identity fraud and an assumption of a duty of care in protecting the individual from identity theft.[113]

51.68 Chartered Secretaries Australia submitted that more specificity was required as to the permitted means of notifying affected individuals of a breach. It noted that a public advertisement may be the most practical, or only, way of notifying certain individuals.[114]

Penalties

51.69 The Australian Taxation Office (ATO) expressed concern about the circumstances in which a civil penalty could be imposed for a failure to notify. It noted that, in cases where an employee had gained access to information inappropriately, there may be some time between when the act took place and the agency becoming aware of the breach. The ATO did not believe an agency should suffer a penalty because notification did not occur quickly.[115] Telstra did not support the availability of a civil penalty for a failure to notify the Privacy Commissioner of a data breach.[116]

Other comments

51.70 A number of organisations argued that the data breach notification schemes should be aligned with other reporting requirements, such as those imposed by the Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA).[117]

51.71 The Cyberspace Law and Policy Centre submitted that the data breach notification provisions should be included in the model UPPs.[118]

51.72 Microsoft submitted that the obligation to notify should apply only to residents of Australia. It argued that if the breach notification obligation applied more broadly, then organisations that do business in multiple jurisdictions are likely to be faced with inconsistent data breach notification obligations that cannot be reconciled.[119]

ALRC's view

51.73 The *Privacy Act* should provide for notification by agencies and organisations to individuals affected by a data breach. This requirement is consistent with the *Privacy*

---

113 Australian Unity Group, *Submission PR 381*, 6 December 2007.
114 Chartered Secretaries Australia, *Submission PR 351*, 28 November 2007.
115 Australian Taxation Office, *Submission PR 515*, 21 December 2007.
116 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
117 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.
118 The ALRC does not agree with this approach, on the basis that the notification requirements are not high-level principles: this is discussed further in Ch 28.
119 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

Act's objective to protect the personal information of individuals. Data breach notification can serve to protect the personal information from any further exposure or misuse, and encourages agencies and organisations to be transparent about their information-handling practices.

51.74 While the data breach notification requirement would operate separately to the requirements for the handling of personal information under the model UPPs,[120] a data breach may occur because an agency or organisation has failed to comply with its obligations in regards to the use and disclosure of personal information,[121] or has failed to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.[122] A data breach, therefore, could be an interference with privacy under the *Privacy Act.*

51.75 A data breach may also occur where an agency or organisation has been in compliance with the *Privacy Act* but the information it holds has been stolen or 'hacked' into. Alternatively, information may have been disclosed due to circumstances that were not foreseeable and, consequently, reasonable steps could not have been taken to prevent the breach.

51.76 Notification requirements are accordingly not reliant on establishing that an agency or organisation has not complied with its data security obligations. Nor are the provisions aimed at 'punishing' bodies when a breach occurs. Rather, the primary rationale for data breach notification laws is that notifying people that their personal information has been breached can help to minimise the damage caused by the breach.[123] Notification acknowledges the fact that a data breach potentially can expose an individual to a serious risk of harm. By arming individuals with the necessary information, they have the opportunity, for example, 'to monitor their accounts, take preventative measures such as new accounts, and be ready to correct any damage done'.[124]

51.77 The view has been put to the ALRC that this rationale does not apply in the case of breaches by financial services institutions. It has been suggested that it is the bank (or other financial institution), not the customer, that is at risk of loss if unauthorised transactions are made to the customer's account. It is the bank, not the customer that would be able to mitigate the potential damage. In the ALRC's view, while it may be the financial institution that mitigates the financial damage, there has still been unauthorised access to the customer's personal information. This access may occasion

---

120 Rec 18–2.

121 See 'Use and Disclosure' principle set out at the front of this Report.

122 See 'Data Security' principle set out at the front of this Report.

123 See M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

124 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 3.

other non-financial risks. One of the fundamental principles underpinning the *Privacy Act* is that an individual should be informed about what happens to his or her personal information.[125]

51.78 While the loss of financial information—and the subsequent risk of identity theft and fraud—clearly is a concern, risks arising from data breaches are not limited to financial harm. Other types of personal information, such as health information, if disclosed, could subject a person to discriminatory treatment or damage to his or her reputation. Informing a person that such information has been disclosed makes that person aware of what may be the possible consequences of the breach.[126]

51.79 The legal requirement to notify in the case of serious breaches is necessary because, as explained above, there is a risk that the uncontrolled market may 'undersupply notification'.[127] That is, because of the reputational damage to organisations that notification can cause, organisations may not have sufficient incentives to notify customers voluntarily of a data breach.[128]

51.80 A data breach notification requirement also can provide incentives to improve data security. The reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful incentives to improve security.

51.81 Notification also plays an important role in keeping the market informed of the privacy practices of organisations. As Professor Robert Baldwin and Professor Martin Cave suggest, 'competitive markets can only function properly if consumers are sufficiently well informed to evaluate competing products'.[129] In the absence of notification, a data breach causes an 'information inadequacy', as the organisation knows that there has been an unauthorised acquisition of an individual's personal information, but the individual affected does not. Until the individual is notified of a data breach, therefore, there may be inadequate information in the market for individuals to evaluate the different information-handling practices of organisations.

51.82 Some organisations already may be subject to notification requirements under other federal legislation. For example, under s 912D of the *Corporations Act 2001* (Cth),[130] a financial services licensee is required to notify ASIC where it has breached, or is likely to breach, certain obligations under the Act. Notification is required only

---

125 Australian Government Office of the Federal Privacy Commissioner Consultation Paper—Draft Voluntary Information Security Breach Notification Guide (2008), 18.

126 Law Council of Australia, Submission PR 527, 21 December 2007.

127 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 13.

128 Ibid, 11.

129 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 12.

130 See also *Superannuation Industry (Supervision) Act 1993* (Cth) s 29J.

where the breach, or likely breach, is significant.[131] While the ALRC notes concerns from stakeholders about adding another notification obligation, these requirements are to notify the regulator of breaches under the relevant Acts, not an individual who may be affected by the breach. In addition, these obligations are concerned with ensuring good corporate governance,[132] and not protecting the privacy of individuals.

Trigger for notification

Real risk of serious harm

51.83 The recommended data breach notification provisions should include a general requirement 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.

51.84 There are several factors to note about this recommended triggering event. First, it sets a higher threshold for notification than is provided in most other tests. Rather than requiring notification of 'any unauthorised acquisition' of personal information, the recommended test allows the agency or organisation to investigate the data breach and make an assessment of whether the unauthorised acquisition may give rise to a real risk of serious harm to an individual. Serious harm is not limited to identity theft or fraud. The harm could include, for example, discrimination, if sensitive medical information was released.

51.85 In international law, the term 'a real risk of serious harm' has been defined to mean 'a reasonable degree of likelihood', 'real and substantial danger' and 'a real and substantial risk'.[133] In the OPC's draft Voluntary Information Security Breach Notification Guide, the OPC sets out a number of questions to evaluate the risks associated with the breach, including:

- what personal information is involved (for example, how sensitive is it; could the information be used for fraudulent purposes);
- what is the cause and extent of the breach (for example, is there a risk of ongoing breaches; is the information easily accessible; was the breach deliberate or inadvertent);
- who is affected (for example, how many people; are they people particularly at risk of harm); and

---

131 *Corporations Act 2001* (Cth) s 912D(1)(b).

132 For example, an entity must notify the regulator when a breach may mean the organisation cannot provide the financial services it is licensed to provide or clients may be subject to a loss: Ibid.

133 See *R v Secretary of State for the Home Department, Ex parte Sivakumaran* [1988] AC 958.

- what harm could result (for example, who is the recipient of the information; could the breach lead to fraud, financial loss or humiliation; what impact could the breach have on the organisation or agency concerned).[134]

51.86 Setting a higher threshold to where there is a real risk of serious harm should reduce the risk of 'notification fatigue'—that is, where individuals receive so many notices of data breaches that it becomes difficult for them to assess which ones carry a serious risk of harm and which ones are minor in nature and consequence. A higher threshold for notification also should reduce the compliance burden on agencies and organisations.

51.87 It also is noted that the agency or organisation decides whether the triggering event has occurred. This will allow organisations and agencies to develop their own standards about what constitutes a real risk of serious harm in the context of their own operations.

51.88 The ALRC's recommendation does, however, provide for oversight by the Privacy Commissioner. It is preferable that the decision to notify is made in consultation with the Privacy Commissioner, and that the Commissioner is able to require notification where he or she believes that the unauthorised acquisition gives rise to a real risk of serious harm to any affected individual. This oversight is similar to the model put forward by the CIPPIC and the Canadian Government Standing Committee on Access to Information, Privacy and Ethics. The Privacy Commissioner also could use this oversight power to require that notification be made to other bodies as appropriate, such as the major credit reporting agencies. It is not intended, however, that agencies and organisations consult with the Commissioner in cases where they are sure that the threshold for notification is not met.

51.89 The requirement to consult with the Privacy Commissioner on whether notification is required also will alert the Commissioner to possible systemic problems within an agency or organisation. Where an agency or organisation has notified the Commissioner of a number of breaches, the Commissioner may consider whether to investigate the matter on his or her own motion.[135] The Commissioner also may use multiple breach notifications as an indication that a Privacy Performance Assessment[136] would be appropriate.

---

134 Australian Government Office of the Federal Privacy Commissioner Consultation Paper—Draft Voluntary Information Security Breach Notification Guide (2008), 23–25.

135 See Chs 49, 50.

136 See Ch 47.

51.90 Consistently with the ALRC's view that the *Privacy Act* be technology neutral,[137] the requirement to notify should not be restricted to computerised information, but should apply to any unauthorised access to personal information—whether through a lost laptop; a hacker accessing electronic files; misplaced hard copy files; or careless disposal of hard copy personal information. This broad application should encourage compliance with the 'Data Security' principle.

Exceptions to notification

51.91 While the recommended triggering event set out above is narrower than that adopted in many states in the US, the ALRC acknowledges the concern expressed by stakeholders that there should be some discretion concerning the requirement to notify. There should also be clear examples of circumstances that are not likely to give rise to a real risk of serious harm. In DP 72, the ALRC took the approach that these examples should be listed as exceptions to the requirement to notify. Following comments made in submissions, the ALRC's view is that these factors should be included as part of the assessment of whether there is a real risk of serious harm arising from the breach.

51.92 First, the provisions should state that, in determining whether there is a real risk of serious harm, consideration should be given to whether the specified personal information was encrypted adequately. The requirement that encryption be 'adequate' implicitly requires that the encryption key was not also acquired by the unauthorised person. In other words, encryption will not be adequate where there is an easy means of decoding the information. This phrasing also avoids any need to specify exactly what type of encryption is adequate. An assessment of adequacy will depend on the circumstances of the case, taking into account matters such as the type of personal information, the nature of the agency or organisation holding it, and the risk of harm that would be caused by its unauthorised acquisition. The Privacy Commissioner should issue guidance on the type and standard of encryption he or she generally will consider adequate.

51.93 The data breach notification provisions should provide that consideration be given to whether the information was acquired in good faith by an employee or agent, where the agency or organisation was otherwise acting for a purpose permitted by the model UPPs—provided that the personal information is not used or subject to further unauthorised disclosure. This would apply to situations where, for example, an employee accidentally gains unauthorised access to personal information of a customer in the process of collecting information for a permitted purpose. It would not cover situations where an employee is acting outside a purpose permitted by the privacy principles, such as where he or she is 'snooping' or accessing personal information for illegitimate purposes.[138] In those circumstances, however, the agency, organisation or Privacy Commissioner would still need to assess whether the unauthorised acquisition

---

137 See Ch 10.

138 See, eg, the 'Centrelink Staff Sacked over Breaches', *Sydney Morning Herald* (online), 22 August 2006, <www.smh.com.au>.

gave rise to a real risk of serious harm to the affected individual. If the information was not disclosed beyond the staff member, then it may be that there is no requirement to notify the affected individual.

51.94 The Privacy Commissioner should have a broad discretion to waive the notification requirement where the Commissioner does not consider that it would be in the public interest to notify. This would cover situations, for example, where there is a law enforcement investigation being undertaken into the breach and notification would impede that investigation, or where the information concerned matters of national security.[139]

'Specified personal information' for the purposes of notification

51.95 In US state data breach notification laws, only the combination of particular types of personal information gives rise to the obligation to notify. The US laws do not apply to the range of personal information which falls within the definition of 'personal information' in the *Privacy Act*.

51.96 The *Privacy Act* should adopt a definition of 'specified personal information' for the purposes of the data breach notification provisions. This definition should draw on the existing definitions of 'personal information' and 'sensitive information' in the *Privacy Act* and should prescribe what combinations of these types of information would, when acquired without authorisation, give rise to a real risk of serious harm requiring notification.

51.97 For example, adopting the approach of the US Interagency Guidance and CIPPIC definitions, 'specified personal information' could include information in electronic or paper form, which includes an individual's name or address, in combination with any of the following:

- driver's licence or proof of age;
- Medicare number—or other unique identifier, such as a tax file number;
- account numbers, credit or debit card numbers, or other unique identifiers issued by other organisations together with any security code, password or access code that would permit access to the individual's information; or

---

139 Examples of when other public interests may outweigh the desirability of protecting privacy are given in other contexts in a number of chapters in this Report. Chapter 65 considers when the public interest in allowing particular research projects to proceed outweighs the public interest in maintaining the level of privacy protection provided by the privacy principles. Chapter 42 discusses the public interest in providing an exemption from the privacy principles for acts and practices conducted in the course of journalism. Chapter 74 considers when acts done in the public interest should be a defence to the statutory cause of action for a serious invasion of privacy.

- sensitive information (as defined in the *Privacy Act*).

51.98 The unauthorised acquisition of such information (whether in combination or alone) could arm a person with sufficient personal information to commit both an 'account takeover' and 'true name fraud', as defined above. The ALRC recognises that this suggested definition of 'specified personal information' is not limited to financial information, as suggested by Microsoft.[140] While preventing identity fraud is one of the key rationales for data breach notification, it is not the only consequence that can flow from an unauthorised acquisition of personal information. Discrimination, stalking, and other harmful consequences potentially could flow from a security breach. The recommended data breach notification provisions, therefore, should deal with more than simply 'sensitive financial information'.

Other matters

51.99 The ALRC has not specified the form, content, method or timing of notification. As with the definition of 'specified personal information', however, there are elements of the US laws and CIPPIC proposal upon which the data breach notification law could be modelled. The model currently under consideration by the Privacy Commissioner in the draft voluntary Guide, as outlined above, is supported by the ALRC.

51.100 At a minimum, the content of breach notification should provide:

- a description of the breach;
- a list of the types of personal information that were disclosed; and
- contact information for affected individuals to obtain more information and assistance.

51.101 The ALRC agrees with the view expressed in submissions that not all agencies and organisations will be able to make an assessment of the risk of identity fraud as a result of the breach, nor will they have expertise in how to mitigate any damage that might flow from the breach. To assist agencies and organisations, the OPC should consider developing, in consultation with relevant bodies such as the AFP, identity theft guidelines.

Method of notification

51.102 Ordinarily, a breach notification should be directed personally to the individual affected. Rather than prescribing the various methods by which an agency or organisation can notify an individual, it would be preferable to allow for the method of notification to be determined by the agency's or organisation's ordinary method of communicating with individuals. If, for example, an agency or organisation usually

140 See Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

corresponds with an individual by post, then it should not provide notification by email. Agencies and organisations also should be able to have regard to any arrangements they have in place for contacting an individual in an emergency situation.

51.103 In relation to substituted notice, the ALRC does not recommend the setting of a particular threshold for allowing substituted notice, in terms of cost of notification or number of people to notify. It would be difficult to set a threshold that would be fair and reasonable to all the agencies and organisations subject to the *Privacy Act*, particularly if the small business exemption were removed.[141] It would be preferable to empower the Privacy Commissioner to approve substituted notice where he or she believes it is appropriate, reasonable and fair in all the circumstances.

Restriction of notification to residents of Australia

51.104 Microsoft has suggested that notification requirements should be restricted to residents of Australia, to avoid companies being subject to a myriad of notification rules across jurisdictions.[142]

51.105 As discussed in Chapter 5, the *Privacy Act* regulates the handling of personal information in Australia by federal departments and agencies, ACT public sector agencies, and private sector organisations, as defined under the Act.[143] The *Privacy Act* also generally applies to an act or practice engaged in outside Australia by an organisation, if the act or practice relates to personal information of an Australian citizen or permanent resident of Australia.[144] For the *Privacy Act* to apply extraterritorially, the organisation must be an Australian citizen; resident; a partnership, trust or body corporate formed in Australia (or an external Territory); or an unincorporated association that has its central management and control in Australia (or an external Territory).[145]

51.106 The general approach of the *Privacy Act* also should apply to the data breach notification provisions. Where a relevant data breach by an agency or organisation occurs within Australia, every affected individual should be notified, regardless of their citizenship or residency status. Where a breach occurs outside Australia by an organisation subject to the extraterritoriality provisions, Australian citizens and permanent residents should be covered by the Australian data breach notification requirements, to the same extent as they are by other protections under the Act.

---

141 See Rec 39–1.
142 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.
143 *Privacy Act 1988* (Cth) s 6C.
144 Ibid s 5B(1). There are some provisions excluded from this general rule which relate to the establishment of tax file number guidelines and credit reporting: J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007), [1–460].
145 *Privacy Act 1988* (Cth) s 5B(2).

Penalties

51.107 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.[146] In cases of serious interferences with privacy, civil financial penalties are likely to be effective against agencies and organisations by providing a strong incentive to comply with the Act. Civil penalties also should be pursued where they would have a worthwhile educative or deterrent effect.

51.108 On this basis, it would be appropriate to allow for a civil penalty to be imposed where an agency or organisation has failed to notify the Privacy Commissioner of a data breach. Such a penalty would provide a strong incentive for agencies and organisations to disclose data breaches where required, and encourage agencies and organisations to consult with the OPC where a data breach has occurred to ensure they are in full compliance with the requirements.[147] The presence of civil penalties also should provide incentives to train staff adequately to, for example, ensure that laptops are not left in airports, hard files are not left unsecured, electronic and hard copy information is disposed of appropriately, and electronic information is encrypted and secured adequately.

51.109 In Chapter 50, the ALRC recommends that the OPC develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty under the *Privacy Act* would be made. In relation to a failure to notify the Commissioner of a data breach, civil penalties should be considered where: there was an apparent blatant disregard of the law; the agency or organisation has a history of previous contraventions of the law; or there was a significant public detriment arising from the breach.

Recommendation 51–1 The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:

(a) 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.

---

146 See also Rec 59–9, which recommends the imposition of a civil penalty for breaches of the credit reporting provisions.

147 See B Arnold, 'Losing It: Corporate Reporting on Data Theft' (2007) 3 *Privacy Law Bulletin* 101, 103.

(b) The definition of 'specified personal information' should include both personal information and sensitive personal information, such as information that combines a person's name and address with a unique identifier, such as a Medicare or account number.

(c) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:

  (i) whether the personal information was encrypted adequately; and

  (ii) whether the personal information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the *Privacy Act* (provided that the personal information is not used or subject to further unauthorised disclosure).

(d) An agency or organisation is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.

(e) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.