Australian Government

Australian Law Reform Commission

For Your Information

Australian Privacy Law and Practice

REPORT

Volume 1
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

Australian Government

Australian Law Reform Commission

The Hon Robert McClelland MP
Attorney-General of Australia
Parliament House
Canberra ACT 2600

30 May 2008

Dear Attorney-General

Review of *Privacy Act 1988*

On 30 January 2006, your predecessor issued terms of reference for the ALRC to undertake a comprehensive review of the *Privacy Act 1988*.

On behalf of the Members of the Commission involved in this Inquiry—including Justice Berna Collier, Justice Robert French, Justice Susan Kenny and Justice Susan Kiefel (until September 2007)—and in accordance with the *Australian Law Reform Commission Act 1996*, we are pleased to present you with the final report in this reference, *For Your Information: Australian Privacy Law and Practice* (ALRC 108, 2008). Owing to the enormous breadth of the subject matter, and the consequent length, this report is presented in three volumes.

Yours sincerely

Professor David Weisbrot AM
President

Professor Les McCrimmon
Commissioner in charge

Professor Rosalind Croucher
Commissioner

Contents

Volume 1

Volume 2

Volume 3

Terms of Reference

REVIEW OF THE PRIVACY ACT 1988

I, Philip Ruddock, Attorney-General of Australia, having regard to:

- the rapid advances in information, communication, storage, surveillance and other relevant technologies
- possible changing community perceptions of privacy and the extent to which it should be protected by legislation
- the expansion of State and Territory legislative activity in relevant areas, and
- emerging areas that may require privacy protection,

refer to the Australian Law Reform Commission for inquiry and report pursuant to subsection 20(1) of the *Australian Law Reform Commission Act 1996*, matters relating to the extent to which the *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia.

1. In performing its functions in relation to this reference, the Commission will consider:

(a) relevant existing and proposed Commonwealth, State and Territory laws and practices

(b) other recent reviews of the *Privacy Act 1988*

(c) current and emerging international law and obligations in this area

(d) privacy regimes, developments and trends in other jurisdictions

(e) any relevant constitutional issue

(f) the need of individuals for privacy protection in an evolving technological environment

(g) the desirability of minimising the regulatory burden on business in this area, and

(h) any other related matter.

2. The Commission will identify and consult with relevant stakeholders, including the Office of the Federal Privacy Commissioner, relevant State and Territory bodies and the Australian business community, and ensure widespread public consultation.

3. The Commission is to report no later than 31 March 2008.*

Dated 30th January 2006

[signed]

Philip Ruddock

Attorney-General

* In a letter dated 11 February 2008, the Attorney-General of Australia, the Hon Robert McClelland MP, agreed to extend the reporting date for the Inquiry to 30 May 2008.

List of Participants

Australian Law Reform Commission

Division

The Division of the ALRC constituted under the *Australian Law Reform Commission Act 1996* (Cth) for the purposes of this Inquiry comprises the following:

Professor David Weisbrot (President)
Professor Les McCrimmon (Commissioner in charge)
Professor Rosalind Croucher (Commissioner) (from February 2007)
Justice Berna Collier (part-time Commissioner) (from October 2007)
Justice Robert French (part-time Commissioner) (from July 2006)
Justice Susan Kenny (part-time Commissioner)
Justice Susan Kiefel (part-time Commissioner) (until September 2007)

Senior Legal Officers

Carolyn Adams
Bruce Alston
Kate Connors (until December 2006 and from January 2008)
Isabella Cosenza (until December 2006 and from January 2008)
Jonathan Dobinson
Alex O'Mara (from February 2008)

Legal Officers

Lisa Eckstein (from August 2007)
Althea Gibson (until March 2007 and from March 2008)
Lauren Jamieson (until January 2008)
Huette Lam
Erin Mackay (from March 2007)
Edward Santow (until December 2007)
Peter Turner (until August 2006)

Research Manager

Lani Blackman

Librarian

Carolyn Kearney

Project Assistants

Alayne Harland
Tina O'Brien

Legal Interns

Megan Caristo
Justin Carter
Elizabeth Crook
Joash Dache
Maggie Fung
Kirsty Hughes
Dawnie Lam
Miranda Lello
Robert Mullins
Danni Nicholas-Sexton
Elnaz Nikibin
Michael Ostroff
Christina Raymond
Fiona Roughley
Teneille Steptoe
Keelyann Thomson
Christina Trahanas
Michelle Tse
Jocelyn Williams
SooJin Yoon

Advisory Committee Members

Dr Bridget Bainbridge, National E-Health Transition Authority
Ms Robin Banks, Public Interest Advocacy Centre
Mr Paul Chadwick, Consultant (formerly Victorian Privacy Commissioner) (until January 2007)
Ms Karen Curtis, Privacy Commissioner
Mr Peter Ford, Privacy, Security and Telecommunications Consultant
Mr Ian Gilbert, Australian Bankers' Association
Mr Duncan Giles, Freehills Solicitors
Professor Margaret Jackson, School of Accounting and Law, RMIT University
Ms Helen Lewin, Telstra Corporation
Associate Professor Roger Magnusson, Faculty of Law, University of Sydney
Associate Professor Moira Paterson, Faculty of Law, Monash University
Ms Joan Sheedy, Privacy and FOI Policy Branch, Department of the Prime Minister and Cabinet
Mr Peter Shoyer, Executive Director of Court Support & Independent Offices, Department of Justice (NT) (formerly Northern Territory Information Commissioner)

Professor Colin Thomson, National Health and Medical Research Council
Mr Nigel Waters, Pacific Privacy Consulting
Ms Beth Wilson, Health Services Commissioner (Vic)
Ms Sue Vardon, Department for Families and Communities (SA)

Credit Reporting Advisory Sub–Committee

Ms Carolyn Bond, Consumer Action Law Centre
Ms Christine Christian, Dun and Bradstreet Pty Ltd
Ms Karen Cox, Consumer Credit Legal Centre (NSW)
Mr Ian Gilbert, Australian Bankers' Association
Ms Helen Gordon, Australian Finance Conference
Mr David Grafton, Commonwealth Bank of Australia
Ms Erica Hughes, Veda Advantage (from September 2007)
Ms Loretta Kreet, Legal Aid Queensland
Mr Andrew Want, Veda Advantage (until September 2007)
Mr Nigel Waters, Pacific Privacy Consulting
Ms Kerstin Wijeyewardene, Department of the Treasury (Cth)

Developing Technology Advisory Sub–Committee

Mr Paul Budde, Managing Director, BuddeComm
Professor William Caelli, Director Information Assurance, International Information Security Consultants Pty Ltd and Faculty of Information Technology, QUT
Mr Chris Cheah, Australian Communications and Media Authority
Professor Peter Croll, Professor of Software Engineering, Faculty of Information Technology, QUT
Mr Malcolm Crompton, Information Integrity Solutions Pty Ltd
Professor Graham Greenleaf, Faculty of Law, University of New South Wales
Professor Margaret Jackson, School of Accounting and Law, RMIT University
Mr David Jonas, Convergence e-Business Solutions Pty Ltd
Mr Greg Stone, National Technology Officer, Microsoft Pty Ltd
Mr Martin Stewart-Weeks, Internet Business Solutions Group, Cisco Systems Australia Pty Ltd
Professor Michael Wagner, National Centre for Biometric Studies, University of Canberra
Mr Stephen Wilson, Lockstep Consulting

Health Advisory Sub–Committee

Ms Amanda Adrian, Australian Nursing Federation
Ms Melanie Cantwell, Consumers' Health Forum of Australia Inc
Professor David Hill, The Cancer Council (Vic)
Ms Anna Johnston, Australian Privacy Foundation
Dr Graeme Miller, Family Medicine Research Centre
Ms Julia Nesbitt, Australian Medical Association (until September 2007)
Professor Margaret Otlowski, Faculty of Law, University of Tasmania

Ms Dianne Scott, Department of Human Services (Vic)
Dr Heather Wellington, Peter MacCallum Cancer Centre

List of Recommendations

Part A—Introduction

3. Achieving National Consistency

Recommendation 3–1 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

(a) *Health Records and Information Privacy Act 2002* (NSW);

(b) *Health Records Act 2001* (Vic);

(c) *Health Records (Privacy and Access) Act 1997* (ACT); and

(d) any other laws prescribed in the regulations.

Recommendation 3–2 States and territories with information privacy legislation that purports to apply to organisations should amend that legislation so that it no longer applies to organisations.

Recommendation 3–3 The *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'preserved matters' set out in the Act. The Australian Government, in consultation with state and territory governments, should develop a list of 'preserved matters'. The list should only include matters that are not covered adequately by an exception to the model Unified Privacy Principles or an exemption under the *Privacy Act*.

Recommendation 3–4 The Australian Government and state and territory governments, should develop and adopt an intergovernmental agreement in relation to the handling of personal information. This agreement should establish an intergovernmental cooperative scheme that provides that the states and territories should enact legislation regulating the handling of personal information in the state and territory public sectors that:

(a) applies the model Unified Privacy Principles (UPPs), any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act* as in force from time to time; and

(b) contains provisions that are consistent with the *Privacy Act*, including at a minimum provisions:

(i) allowing Public Interest Determinations and Temporary Public Interest Determinations;

(ii) regulating state and territory incorporated bodies (including statutory corporations);

(iii) regulating state and territory government contracts;

(iv) regulating data breach notification; and

(v) regulating decision making by individuals under the age of 18.

Recommendation 3–5 To promote and maintain uniformity, the Standing Committee of Attorneys-General (SCAG) should adopt an intergovernmental agreement which provides that any proposed changes to the:

(a) model Unified Privacy Principles and relevant definitions used in the *Privacy Act* must be approved by SCAG; and

(b) new *Privacy (Health Information) Regulations* and relevant definitions must be approved by SCAG, in consultation with the Australian Health Ministers' Conference.

The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

Recommendation 3–6 The Australian Government should 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.

5. The *Privacy Act*: Name, Structure and Objects

Recommendation 5–1 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 model Unified Privacy Principles (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.

Recommendation 5–2 The *Privacy Act* should be redrafted to achieve greater logical consistency, simplicity and clarity.

Recommendation 5–3 The *Privacy Act* should be renamed the *Privacy and Personal Information Act*. If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, however, the name of the Act should remain the same.

Recommendation 5–4 The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be specified to:

(a) implement, in part, Australia's obligations at international law in relation to privacy;

(b) recognise that individuals have a right to privacy and to promote the protection of that right;

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests;

(d) provide the basis for nationally consistent regulation of privacy and the handling of personal information;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy;

(g) establish the Australian Privacy Commission and the position of the Privacy Commissioner; and

(h) provide an avenue for individuals to seek redress when there has been an alleged interference with their privacy.

6. The *Privacy Act*: Some Important Definitions

Recommendation 6–1 The *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

Recommendation 6–2 The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'identified or reasonably identifiable'.

Recommendation 6–3 The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'not reasonably identifiable'.

Recommendation 6–4 The definition of 'sensitive information' in the *Privacy Act* should be amended to include:

(a) biometric information collected for the purpose of automated biometric verification or identification; and

(b) biometric template information.

Recommendation 6–5 The definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual preferences and practices'.

Recommendation 6–6 The definition of 'record' in the *Privacy Act* should be amended to make clear that a record includes:

(a) a document (as defined in the *Acts Interpretation Act 1901* (Cth)); and

(b) information stored in electronic or other format.

Recommendation 6–7 The definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.

7. Privacy Beyond the Individual

Recommendation 7–1 The Office of the Privacy Commissioner should encourage and assist agencies and organisations to develop and publish protocols, in consultation with Indigenous groups and representatives, to address the particular privacy needs of Indigenous groups.

Recommendation 7–2 The Australian Government should undertake an inquiry to consider whether legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take.

8. Privacy of Deceased Individuals

Recommendation 8–1 The *Privacy Act* should be amended to include provisions dealing with the personal information of individuals who have been dead for 30 years or less where the information is held by an organisation. The Act should provide as follows:

(a) Use and Disclosure

Organisations should be required to comply with the 'Use and Disclosure' principle in relation to the personal information of deceased individuals. Where the principle would have required consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. The organisation must not use or disclose the information if the use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

(b) Access

Organisations should be required to provide third parties with access to the personal information of deceased individuals in accordance with the access elements of the 'Access and Correction' principle, except to the extent that providing access would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

(c) Data Quality

Organisations should be required to comply with the use and disclosure elements of the 'Data Quality' principle in relation to the personal information of deceased individuals.

(d) Data Security

Organisations should be required to comply with the 'Data Security' principle in relation to the personal information of deceased individuals.

Recommendation 8–2 The *Privacy Act* should be amended to provide that the content of National Privacy Principle 2.1(ea) on the use and disclosure of genetic information to genetic relatives—to be moved to the new *Privacy (Health Information) Regulations* in accordance with Recommendation 63–5—should apply to the use and disclosure of genetic information of deceased individuals.

Recommendation 8–3 Breach of the provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner:

(a) in relation to an alleged breach of the use and disclosure, access, data quality or data security provisions—the deceased individual's parent, child or sibling who is aged 18 or over, spouse, de facto partner or legal personal representative; and

(b) in relation to an alleged breach of the access provision—the parties in paragraph (a) and any person who has made a request for access to the personal information of a deceased individual where that request has been denied.

Part B—Developing Technology

10. Accommodating Developing Technology in a Regulatory Framework

Recommendation 10–1 In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations.

Recommendation 10–2 The Office of the Privacy Commissioner should develop and publish educational materials for individuals, agencies and organisations about specific privacy-enhancing technologies and the privacy-enhancing ways in which technologies can be deployed.

Recommendation 10–3 The Office of the Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy. This guidance should incorporate relevant local and international standards. Matters that such guidance should address include:

(a) developing technologies such as radio frequency identification (RFID) or data-collecting software such as 'cookies';

(b) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';

(c) when the use of a certain technology will require agencies and organisations to notify individuals at or before the time of collection of personal information;

(d) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometric systems);

(e) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information in an intelligible form (for example, the type of biometric information that is held as a biometric template); and

(f) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.

Recommendation 10–4 The Office of the Privacy Commissioner should develop and publish guidance for organisations on the privacy implications of data-matching.

11. Individuals, the Internet and Generally Available Publications

Recommendation 11–1 The Office of the Privacy Commissioner should develop and publish guidance that relates to generally available publications in an electronic format. This guidance should:

(a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;

(b) set out the factors that agencies and organisations should consider before publishing personal information in an electronic format (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and

(c) clarify the application of the model Unified Privacy Principles to the collection of personal information from generally available publications for inclusion in a record or another generally available publication.

Recommendation 11–2 The Australian Government should ensure that federal legislative instruments establishing public registers containing personal information set out clearly any restrictions on the electronic publication of that information.

Part C—Interaction, Inconsistency and Fragmentation

14. The Costs of Inconsistency and Fragmentation

Recommendation 14–1 Agencies that are required or authorised by legislation, a code or a Public Interest Determination to share personal information should, where appropriate, develop and publish documentation that addresses the sharing of personal information; and publish other documents (including memorandums of understanding and ministerial agreements) relating to the sharing of personal information.

Recommendation 14–2 The Australian Government, in consultation with: state and territory governments; intelligence agencies; law enforcement agencies; and accountability bodies, including the Office of the Privacy Commissioner, the Inspector-General of Intelligence and Security, the Australian Commission for Law Enforcement

Integrity, state and territory privacy commissioners and agencies with responsibility for privacy regulation, and federal, state and territory ombudsmen, should:

(a) develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

(b) develop memorandums of understanding to clarify the existing roles of accountability bodies that oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.

15. Federal Information Laws

Recommendation 15–1 The *Freedom of Information Act 1982* (Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act* is a disclosure that is required or authorised by or under law for the purposes of the 'Use and Disclosure' principle under the *Privacy Act*.

Recommendation 15–2 The Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.

Recommendation 15–3 Part VIII of the *Privacy Act* (Obligations of confidence) should be repealed.

16. Required or Authorised by or Under Law

Recommendation 16–1 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:

(a) Commonwealth, state and territory Acts and delegated legislation;

(b) a duty of confidentiality under common law or equity (including any exceptions to such a duty);

(c) an order of a court or tribunal; and

(d) documents that are given the force of law by an Act, such as industrial awards.

Recommendation 16–2 The Office of the Privacy Commissioner should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. This guidance should include:

(a) a list of examples of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*; and

(b) a note to the effect that the list is intended to be a guide only and that omission from the list does not mean that a particular law cannot be relied upon for the purposes of a 'required or authorised by or under law' exception in the model Unified Privacy Principles.

Recommendation 16–3 The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, state and territory privacy commissioners and agencies with responsibility for privacy regulation, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

Recommendation 16–4 The review under s 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) should consider, in particular, whether:

(a) reporting entities and designated agencies are handling personal information appropriately under the legislation;

(b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;

(c) it remains appropriate that reporting entities are required to retain information for seven years;

(d) the use of the electoral roll by reporting entities for the purpose of identification verification is appropriate; and

(e) the handling of information by the Australian Transaction Reports and Analysis Centre is appropriate, particularly as it relates to the provision of access to other bodies, including bodies outside Australia.

17. Interaction with State and Territory Laws

Recommendation 17–1 When an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies that handle personal information, the Australian Government agency should ensure that a memorandum of understanding or other arrangement is in place to provide for the appropriate handling of personal information.

Recommendation 17–2 State and territory privacy legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

Recommendation 17–3 The Office of the Privacy Commissioner should develop and publish memorandums of understanding with each of the bodies with responsibility for information privacy in Australia, including state and territory bodies and external dispute resolution bodies with responsibility for privacy. These memorandums of understanding should outline:

(a) the roles and functions of each of the bodies;

(b) when a matter will be referred to, or received from, each of the bodies;

(c) processes for consultation between the bodies when issuing Public Interest Determinations and Temporary Public Interest Determinations, approving codes and developing rules; and

(d) processes for developing and publishing joint guidance.

Part D—The Privacy Principles

18. Structural Reform of the Privacy Principles

Recommendation 18–1 The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:

(a) the obligations in the privacy principles generally should be expressed as high-level principles;

(b) the privacy principles should be technology neutral;

(c) the privacy principles should be simple, clear and easy to understand and apply; and

(d) the privacy principles should impose reasonable obligations on agencies and organisations.

Recommendation 18–2 The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles, referred to in this Report as the model Unified Privacy Principles.

19. Consent

Recommendation 19–1 The Office of the Privacy Commissioner should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should:

(a) address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained;

(b) cover express and implied consent as it applies in various contexts; and

(c) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

20. Anonymity and Pseudonymity

Recommendation 20–1 The model Unified Privacy Principles should contain a principle called 'Anonymity and Pseudonymity' that requires an agency or organisation to give individuals the clear option to interact anonymously or pseudonymously, where this is lawful and practicable in the circumstances.

Recommendation 20–2 The Office of the Privacy Commissioner should develop and publish guidance on:

(a) when it is and is not 'lawful and practicable' to give individuals the option to interact anonymously or pseudonymously with agencies or organisations;

(b) what is involved in providing a 'clear option' to interact anonymously or pseudonymously; and

(c) the difference between providing individuals with the option to interact anonymously and pseudonymously.

21. Collection

Recommendation 21–1 The model Unified Privacy Principles should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.

Recommendation 21–2 The Office of the Privacy Commissioner should develop and publish further guidance to clarify when it would not be reasonable and

practicable to collect personal information about an individual only from the individual concerned. In particular, the guidance should address collection:

(a) of personal information by agencies pursuant to the exercise of their coercive information-gathering powers or in accordance with their intelligence-gathering, investigative, and compliance functions;

(b) of statistical data;

(c) of personal information in circumstances in which it is necessary to verify an individual's personal information;

(d) of personal information in circumstances in which the collection process is likely to, or will, disclose the personal information of multiple individuals; and

(e) from persons under the age of 18, persons with a decision-making incapacity and those authorised to provide personal information on behalf of the individual.

Recommendation 21–3 The 'Collection' principle should provide that, where an agency or organisation receives unsolicited personal information, it must either:

(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 model Unified Privacy Principles that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

Recommendation 21–4 The Office of the Privacy Commissioner should develop and publish guidance about the meaning of 'unsolicited' in the context of the 'Collection' principle.

Recommendation 21–5 The 'Collection' principle in the model Unified Privacy Principles should provide that an agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

22. Sensitive Information

Recommendation 22–1 The model Unified Privacy Principles should set out the requirements of agencies and organisations in relation to the collection of personal information that is defined as 'sensitive information' for the purposes of the *Privacy Act*. These requirements should be located in the 'Collection' principle.

Recommendation 22–2 The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or authorised by or under law.

Recommendation 22–3 The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is legally or physically incapable of giving or communicating consent.

23. Notification

Recommendation 23–1 The model Unified Privacy Principles should contain a principle called 'Notification' that sets out the requirements on agencies and organisations to notify individuals or otherwise ensure they are aware of particular matters relating to the collection and handling of personal information about the individual.

Recommendation 23–2 The 'Notification' principle should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify or otherwise ensure that the individual is aware of the:

(a) fact and circumstances of collection where the individual may not be aware that his or her personal information has been collected;

(b) identity and contact details of the agency or organisation;

(c) rights of access to, and correction of, personal information provided by these principles;

(d) purposes for which the information has been collected;

(e) main consequences of not providing the information;

(f) actual, or types of, agencies, organisations, entities or persons to whom the agency or organisation usually discloses personal information of the kind collected;

(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and

(h) fact, where applicable, that the collection is required or authorised by or under law.

Recommendation 23–3 The Office of the Privacy Commissioner should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. In particular, the guidance should address:

(a) the circumstances when it would and would not be reasonable for an agency or organisation to take no steps to notify individuals about the matters specified in the 'Notification' principle. In this regard, the guidance should address the circumstances when:

(i) notification would prejudice the purpose of collection, for example, where it would prejudice:

- the prevention, detection, investigation, and prosecution of offences, breaches of law imposing a penalty or seriously improper conduct;

- the enforcement of laws; or

- the protection of the public revenue;

(ii) the collection of personal information is required or authorised by or under law for statistical or research purposes;

(iii) the personal information is collected from an individual on repeated occasions;

(iv) an individual has been made aware of the relevant matters by the agency or organisation which disclosed the information to the collecting agency or organisation;

(v) non-compliance with the principle is authorised by the individual concerned;

(vi) the taking of no steps is required or authorised by or under law;

(vii) notification would pose a serious threat to the life or health of any individual; and

(viii) health services collect family, social or medical histories;

(b) the appropriate level of specificity when notifying individuals about anticipated disclosures to agencies, organisations, entities and persons; and

(c) the circumstances in which an agency or organisation can comply with specific limbs of the 'Notification' principle by alerting an individual to specific sections of its Privacy Policy or to other general documents.

24. Openness

Recommendation 24–1 The model Unified Privacy Principles should contain a principle called 'Openness'. The principle should set out the requirements on an agency or organisation to operate openly and transparently by setting out clearly expressed policies on its handling of personal information in a Privacy Policy, including how it collects, holds, uses and discloses personal information. This document also should include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the steps individuals may take to access and correct personal information about them held by the agency or organisation; and

(d) the avenues of complaint available to individuals in the event that they have a privacy complaint.

Recommendation 24–2 An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the 'Openness' principle, available without charge to an individual electronically; and, on request, in hard copy or in an alternative form accessible to individuals with special needs.

Recommendation 24–3 The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information-handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.

25. Use and Disclosure

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.

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.

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.

26. Direct Marketing

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.

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.

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

(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.

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.

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.

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.

27. Data Quality

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.

28. Data Security

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.

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.

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).

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.

29. Access and Correction

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.

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.

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.

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.

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.

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:

(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.

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.

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.

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

(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.

30. Identifiers

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 regulation-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.

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.

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).

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.

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.

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*.

31. Cross-border Data Flows

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.

(b) The model Unified Privacy Principles should contain a principle called 'Cross-border Data Flows' that applies to agencies and organisations.

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.

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.

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.

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.

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.

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.

Part E—Exemptions

33. Overview: Exemptions from the *Privacy Act*

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

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.

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

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.

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.

36. Exempt Agencies under the *Freedom of Information Act*

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.

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

(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

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.

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.

(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.

38. Other Public Sector Exemptions

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.

39. Small Business Exemption

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.

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

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.

41. Political Exemption

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.

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).

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

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.

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.

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.

44. New Exemptions or Exceptions

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*.

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.

Part F—Office of the Privacy Commissioner

46. Structure of the Office of the Privacy Commissioner

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.

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.

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'.

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

Recommendation 47–1 The *Privacy Act* should be amended to delete the word 'computer' from s 27(1)(c).

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*:

(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*.

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.

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.

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.

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.

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.

48. Privacy Codes

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

(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.

49. Investigation and Resolution of Privacy Complaints

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.

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.

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.

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.

(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.

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.

Recommendation 49–8 The Office of the Privacy Commissioner should develop and publish a document setting out its complaint-handling policies and procedures.

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.

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.

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.

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*

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.

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.

51. Data Breach Notification

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.

(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.

Part G—Credit Reporting Provisions

54. Approach to Reform

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

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

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

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

(b) held by a credit provider; and

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

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

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

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

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

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

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

Recommendation 54–9 Credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, should develop a credit reporting code providing detailed guidance within the framework provided by the *Privacy Act* and the new *Privacy (Credit Reporting Information) Regulations.* The credit reporting code should deal with a range of operational matters relevant to compliance.

55. More Comprehensive Credit Reporting

Recommendation 55–1 The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include the following categories of personal information, in addition to those currently permitted in credit information files under the *Privacy Act*:

(a) the type of each credit account opened (for example, mortgage, personal loan, credit card);

(b) the date on which each credit account was opened;

(c) the current limit of each open credit account; and

(d) the date on which each credit account was closed.

Recommendation 55–2 Subject to Recommendation 55–3, the new *Privacy (Credit Reporting Information) Regulations* should also permit credit reporting information to include an individual's repayment performance history, comprised of information indicating:

(a) whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not,

(b) the number of repayment cycles the individual was in arrears.

Recommendation 55–3 The Australian Government should implement Recommendation 55–2 only after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

Recommendation 55–4 The credit reporting code should set out procedures for reporting repayment performance history, within the parameters prescribed by the new *Privacy (Credit Reporting Information) Regulations*.

Recommendation 55–5 The new Privacy *(Credit Reporting Information) Regulations* should provide for the deletion of the information referred to in Recommendation 55–1 two years after the date on which a credit account is closed.

56. Collection and Permitted Content of Credit Reporting Information

Recommendation 56–1 The new *Privacy (Credit Reporting Information) Regulations* should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information. This list

should be based on the provisions of s 18E of the *Privacy Act*, subject to the changes set out in Recommendations 55–1, 55–2, 56–2 to 56–4, 56–6, 56–8 and 56–9.

Recommendation 56–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies are not permitted to list overdue payments of less than a prescribed amount.

Recommendation 56–3 The new *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques.

Recommendation 56–4 The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index administered under the *Bankruptcy Regulations 1966* (Cth).

Recommendation 56–5 Credit reporting agencies should ensure that credit reports adequately differentiate the forms of administration identified on the National Personal Insolvency Index (NPII); and accurately reflect the relevant information recorded on the NPII, as updated from time to time.

Recommendation 56–6 The new *Privacy (Credit Reporting Information) Regulations* should allow for the listing of a 'serious credit infringement' based on the definition currently set out in s 18E(1)(b)(x) of the *Privacy Act*, amended so that the credit provider is required to have taken reasonable steps to contact the individual before reporting a serious credit infringement under s 18E(1)(b)(x)(c).

Recommendation 56–7 The Office of the Privacy Commissioner should develop and publish guidance on the criteria that need to be satisfied before a serious credit infringement may be listed, including:

(a) how to interpret 'serious' (for example, in terms of the individual's conduct, and the period and amount of overdue payments);

(b) how to establish whether reasonable steps to contact the individual have been taken;

(c) whether a serious credit infringement should be listed where there is a dispute between the parties that is subject to dispute resolution; and

(d) the obligations on credit providers and individuals in proving or disproving that a serious credit infringement has occurred.

Recommendation 56–8 The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as defined in the *Privacy Act*.

Recommendation 56–9 The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals who the credit provider or credit reporting agency knows, or reasonably should know, to be under the age of 18.

Recommendation 56–10 The new *Privacy (Credit Reporting Information) Regulations* should provide, in addition to the other provisions of the 'Notification' principle, that at or before the time personal information to be disclosed to a credit reporting agency is collected about an individual, a credit provider must take such steps as are reasonable, if any, to ensure that the individual is aware of the:

(a) identity and contact details of the credit reporting agency;

(b) rights of access to, and correction of, credit reporting information provided by the regulations; and

(c) actual or types of organisations, agencies, entities or persons to whom the credit reporting agency usually discloses credit reporting information.

Recommendation 56–11 The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit provider, before disclosing overdue payment information to a credit reporting agency, must have taken reasonable steps to ensure that the individual concerned is aware of the intention to report the information. Overdue payment information, for these purposes, means the information currently referred to in s 18E(b)(1)(vi) of the *Privacy Act.*

57. Use and Disclosure of Credit Reporting Information

Recommendation 57–1 The new *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information. This list should be based on the provisions of Part IIIA of the *Privacy Act*, which currently authorise the use and disclosure by credit reporting agencies and credit providers of personal information contained in credit information files, credit reports and reports relating to credit worthiness (ss 18L, 18K and 18N).

Recommendation 57–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit reporting agency or credit provider may use or disclose credit reporting information for a secondary purpose related to the assessment of an application for credit or the management of an existing credit account, where the individual concerned would reasonably expect such use or disclosure.

Recommendation 57–3 The new *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing, including the pre-screening of direct marketing lists.

Recommendation 57–4 The use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) should be authorised expressly under the AML/CTF Act.

Recommendation 57–5 The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to prohibit for a specified period the disclosure by a credit reporting agency of credit reporting information about them without their express authorisation.

Recommendation 57–6 There should be no equivalent in the new *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information in 'reports' related to credit worthiness. The use and disclosure limitations should apply only to 'credit reporting information' as defined for the purposes of the new regulations.

58. Data Quality and Security

Recommendation 58–1 The new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a state or a territory from bringing proceedings against the individual to recover the amount of the overdue payment; or where any relevant statutory limitation period has expired.

Recommendation 58–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt—such as by entering into a scheme of arrangement with the credit provider—an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information for the full five-year period permissible under the regulations.

Recommendation 58–3 The credit reporting code should promote data quality by setting out procedures to ensure consistency and accuracy of credit reporting information. These procedures should deal with matters including:

(a) the timeliness of the reporting of credit reporting information;

(b) the calculation of overdue payments for credit reporting purposes;

(c) obligations to prevent the multiple listing of the same debt;

(d) the updating of credit reporting information; and

(e) the linking of credit reporting information relating to individuals who may or may not be the same individual.

Recommendation 58–4 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

(a) enter into agreements with credit providers that contain obligations to ensure the quality and security of credit reporting information;

(b) establish and maintain controls to ensure that only credit reporting information that is accurate, complete and up-to-date is used or disclosed;

(c) monitor data quality and audit compliance with the agreements and controls; and

(d) identify and investigate possible breaches of the agreements and controls.

Recommendation 58–5 The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.

Recommendation 58–6 The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of information about voluntary arrangements with creditors under Parts IX and X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.

59. Access and Correction, Complaint Handling and Penalties

Recommendation 59–1 The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to obtain access to credit reporting information based on the provisions currently set out in s 18H of the *Privacy Act*.

Recommendation 59–2 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must provide individuals, on request, with one free copy of their credit reporting information annually.

Recommendation 59–3 The new *Privacy (Credit Reporting Information) Regulations* should provide an equivalent of s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised for a credit-related purpose by a person authorised in writing.

Recommendation 59–4 The new *Privacy (Credit Reporting Information) Regulations* should provide that, where a credit provider refuses an application for credit based wholly or partly on credit reporting information, it must notify an individual of that fact. These notification requirements should be based on the provisions currently set out in s 18M of the *Privacy Act*.

Recommendation 59–5 The new *Privacy (Credit Reporting Information) Regulations* should provide that:

(a) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint in a fair, efficient and timely manner;

(b) a credit reporting agency should refer to a credit provider for resolution complaints about the content of credit reporting information provided to the agency by that credit provider; and

(c) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint, it must inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

Recommendation 59–6 The new *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given, if an individual's application for credit is refused based wholly or partly on credit reporting information, should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.

Recommendation 59–7 The new *Privacy (Credit Reporting Information) Regulations* should provide that credit providers only may list overdue payment or repayment performance history where the credit provider is a member of an external dispute resolution scheme recognised by the Privacy Commissioner.

Recommendation 59–8 The new *Privacy (Credit Reporting Information) Regulations* should provide that, within 30 days, evidence to substantiate disputed credit reporting information must be provided to the individual, or the matter referred to an external dispute resolution scheme recognised by the Privacy Commissioner. If these requirements are not met, the credit reporting agency must delete or correct the information on the request of the individual concerned.

Recommendation 59–9 The *Privacy Act* should be amended to remove the credit reporting offences and allow a civil penalty to be imposed as provided for by Recommendation 50–2.

Part H—Health Services and Research

60. Regulatory Framework for Health Information

Recommendation 60–1 Health information should be regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles (UPPs), and regulations under the *Privacy Act*—the new *Privacy (Health Information) Regulations*. The new *Privacy (Health Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model UPPs.

Recommendation 60–2 The Office of the Privacy Commissioner should publish a document bringing together the model Unified Privacy Principles (UPPs) and the additions set out in the new *Privacy (Health Information) Regulations*. This document should contain a complete set of the model UPPs as they relate to health information.

Recommendation 60–3 The Office of the Privacy Commissioner—in consultation with the Department of Health and Ageing and other relevant stakeholders—should develop and publish guidelines on the handling of health information under the *Privacy Act* and the new *Privacy (Health Information) Regulations*.

61. Electronic Health Information Systems

Recommendation 61–1 If a national Unique Healthcare Identifiers (UHIs) or a national Shared Electronic Health Records (SEHR) scheme goes forward, it should be established under specific enabling legislation. This legislation should address information privacy issues, such as:

(a) the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;

(b) the eligibility criteria, rights and requirements for participation in the UHI and SEHR schemes by health consumers and health service providers, including consent requirements;

(c) permitted and prohibited uses and linkages of the personal information held in the systems;

(d) permitted and prohibited uses of UHIs and sanctions in relation to misuse; and

(e) safeguards in relation to the use of UHIs, including providing that it is not necessary to use a UHI in order to access health services.

62. The *Privacy Act* and Health Information

Recommendation 62–1 The definition of 'health information' in the *Privacy Act* should be amended to make express reference to the *physical, mental or psychological* health or disability of an individual.

Recommendation 62–2 The *Privacy Act* should be amended to define a 'health service' as:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

  (i) assess, predict, maintain or improve the individual's physical, mental or psychological health or status;

  (ii) diagnose the individual's illness, injury or disability; or

  (iii) prevent or treat the individual's illness, injury or disability or suspected illness, injury or disability;

(b) a health-related disability, palliative care or aged care service;

(c) a surgical or related service; or

(d) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

63. *Privacy (Health Information) Regulations*

Recommendation 63–1 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle, an agency or organisation that provides a health service may collect health information from an individual, or a person responsible for the individual, about third parties when:

(a) the collection of the third party's information is necessary to enable the health service provider to provide a health service directly to the individual; and

(b) the third party's information is relevant to the family, social or medical history of that individual.

Recommendation 63–2 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle, an agency or organisation that is a health service provider may collect health information about an individual if the information is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose.

Recommendation 63–3 National Privacy Principles (NPPs) 2.4 to 2.6—dealing with the disclosure of health information by a health service provider to a person who is responsible for an individual—should be moved to the new *Privacy (Health Information) Regulations*. The new regulations should provide that, in addition to the other provisions of the 'Use and Disclosure' principle, an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual, if the individual is incapable of giving consent to the disclosure and all the other circumstances currently set out in NPP 2.4 are met. In addition, the new regulations should:

(a) be expressed to apply to both agencies and organisations;

(b) not refer to a health service provider who may make a disclosure under these provisions as a 'carer'; and

(c) define 'a person who is responsible for an individual' as:

  (i) a parent, child or sibling of the individual;

  (ii) a spouse or de facto partner of the individual;

  (iii) a relative of the individual who is a member of the individual's household;

  (iv) a substitute decision maker authorised by a federal, state or territory law to make decisions about the individual's health;

  (v) a person who has an intimate personal relationship with the individual;

  (vi) a person nominated by the individual to be contacted in case of emergency; or

  (vii) a person who is primarily responsible for providing support or care to the individual.

In considering whether to disclose an individual's health information to a person who is responsible for an individual and who is under the age of 18, a health service provider should consider, on a case-by-case basis, that person's maturity and capacity to understand the information.

Recommendation 63–4 The *Privacy Act* should be amended to provide a definition of 'de facto partner' in the following terms: 'de facto partner' means a person in a relationship as a couple with another person to whom he or she is not married.

Recommendation 63–5 The new *Privacy (Health Information) Regulations* should include provisions similar to those set out in National Privacy Principle 2.1(ea) on the use and disclosure of genetic information where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. These regulations should apply to both agencies and organisations. Any use or disclosure under the new regulations should be in accordance with rules issued by the Privacy Commissioner.

Recommendation 63–6 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, if an individual is denied access to his or her own health information by an agency on the basis that providing access would, or could reasonably be expected to, endanger the life or physical safety of any person, or by an organisation on the basis that providing access would be reasonably likely to pose a serious threat to the life or health of any individual:

(a) the agency or organisation must advise the individual that he or she may nominate a suitably qualified health service provider ('nominated health service provider') to be given access to the health information;

(b) the individual may nominate a health service provider and request that the agency or organisation provide the nominated health service provider with access to the information;

(c) if the agency or organisation does not object to the nominated health service provider, it must provide the nominated health service provider with access to the health information within a reasonable period of time; and

(d) the nominated health service provider may assess the grounds for denying access to the health information and may provide the individual with access to the information to the extent that the nominated health service provider is satisfied that to do so, in the case of an agency, would not, or could not be reasonably expected to, endanger the life or physical safety of any person and, in the case of an organisation, would not be reasonably likely to pose a serious threat to the life or health of any individual.

If the agency or organisation objects to the nominated health service provider and refuses to provide the nominated health service provider with access to the information, the individual may nominate another suitably qualified health service provider, or may lodge a complaint with the Privacy Commissioner alleging an interference with privacy.

Recommendation 63–7 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Data Security' principle, where an agency or organisation that provides a health service is sold, amalgamated or closed down, and an individual health service provider will not be providing health services in the new agency or organisation, or an individual health service provider dies, the provider, or the legal representative of the provider, must take reasonable steps to:

(a) make individual users of the health service aware of the sale, amalgamation or closure of the health service, or the death of the health service provider; and

(b) inform individual users of the health service about proposed arrangements for the transfer or storage of individuals' health information.

Recommendation 63–8 (a) The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, where an individual requests that an agency or organisation that is a health service provider transfers the individual's health information to another health service provider, the agency or organisation must respond within a reasonable time and transfer the information.

(b) Other elements of the 'Access and Correction' principle relating to access should apply to a request for transfer from one health service provider to another, amended as necessary.

Recommendation 63–9 The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle and the 'Use and Disclosure' principle, an agency or organisation may collect, use or disclose health information where necessary for the funding, management, planning, monitoring, or evaluation of a health service where:

(a) the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual or from which the individual would not be reasonably identifiable;

(b) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and

(c) the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.

Recommendation 63–10 The *Privacy Act* should be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, or evaluation of a health service.

65. Research: Recommendations for Reform

Recommendation 65–1 (a) The Privacy Commissioner should issue one set of rules under the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle to replace the *Guidelines under Section 95 of the Privacy Act 1988* and the *Guidelines Approved under Section 95A of the Privacy Act 1988*.

(b) The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the 'Collection' and 'Use and Disclosure' principles—that is, the 'Research Rules'.

(c) Those elements of the *National Statement on Ethical Conduct in Human Research* dealing with privacy should be aligned with the *Privacy Act* and the Research Rules to minimise confusion for institutions, researchers and Human Research Ethics Committees.

Recommendation 65–2 The *Privacy Act* should be amended to extend the arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

Recommendation 65–3 The *Privacy Act* should be amended to provide that 'research' includes the compilation or analysis of statistics.

Recommendation 65–4 The research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle should provide that, before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*.

Recommendation 65–5 The research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle should include a provision stating that it must be 'unreasonable or impracticable' to seek consent from individuals to the collection, use or disclosure of their personal information before that information may be used without consent for the purposes of research.

Recommendation 65–6 The National Health and Medical Research Council, the Australian Research Council and Universities Australia should amend the *National Statement on Ethical Conduct in Human Research* to state that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by a Human Research Ethics Committee.

Recommendation 65–7 The Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements imposed under the *Privacy Act* on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.

Recommendation 65–8 The research exception to the 'Collection' principle should provide that an agency or organisation may collect personal information, including sensitive information, about an individual where all of the following conditions are met:

(a) the collection is necessary for research;

(b) the purpose cannot be served by the collection of information that does not identify the individual;

(c) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;

(d) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; and

(e) the information is collected in accordance with the Research Rules, to be issued by the Privacy Commissioner.

Where an agency or organisation collects personal information about an individual under this exception, it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Recommendation 65–9 The research exception to the 'Use and Disclosure' principle should provide that an agency or organisation may use or disclose personal information where all of the following conditions are met:

(a) the use or disclosure is necessary for research;

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

(c) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*;

(d) the information is used or disclosed in accordance with the Research Rules, to be issued by the Privacy Commissioner; and

(e) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable.

66. Research: Databases and Data Linkage

Recommendation 66–1 The Privacy Commissioner should address the following matters in the Research Rules:

(a) in what circumstances and under what conditions it is appropriate to collect, use or disclose personal information without consent for inclusion in a database or register for research purposes; and

(b) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

Recommendation 66–2 Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should conduct a Privacy Impact Assessment to ensure that the privacy risks involved are assessed and adequately managed in the design and implementation of the project.

Recommendation 66–3 The Research Rules, to be issued by the Privacy Commissioner, should address the circumstances in which, and the conditions under which, it is appropriate to collect, use or disclose personal information without consent in order to identify potential participants in research.

Part I—Children, Young People and Adults Requiring Assistance

67. Children, Young People and Attitudes to Privacy

Recommendation 67–1 The Australian Government should fund a longitudinal study of the attitudes of Australians, in particular young Australians, to privacy.

Recommendation 67–2 The Office of the Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people.

Recommendation 67–3 The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority, should ensure that specific guidance on the privacy aspects of using social networking websites is developed and incorporated into publicly available educational material.

Recommendation 67–4 In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, including privacy in the online environment, into school curriculums.

68. Decision Making by and for Individuals Under the Age of 18

Recommendation 68–1 The *Privacy Act* should be amended to provide that where it is reasonable and practicable to make an assessment about the capacity of an individual under the age of 18 to give consent, make a request or exercise a right of access under the Act, an assessment about the individual's capacity should be undertaken. Where an assessment of capacity is not reasonable or practicable, then an individual:

(a) aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and

(b) under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access.

Recommendation 68–2 The *Privacy Act* should be amended to provide that where an individual under the age of 18 is assessed or presumed to not have capacity under the Act, any consent, request or exercise of a right in relation to that individual must be provided or made by a person with parental responsibility for the individual.

Recommendation 68–3 The *Privacy Act* should be amended to provide that, in order to rely on the age-based presumption, an agency or organisation is required to take such steps, if any, as are reasonable in the circumstances to verify that the individual is aged 15 or over.

Recommendation 68–4 The Office of the Privacy Commissioner should develop and publish guidance for applying the new provisions of the *Privacy Act* relating to individuals under the age of 18, including on:

(a) the involvement of children, young people and persons with parental responsibility in decision-making processes;

(b) situations in which it is reasonable and practicable to make an assessment regarding capacity of children and young people;

(c) practices and criteria to be used in determining whether a child or young person is capable of giving consent, making a request or exercising a right on his or her own behalf, including reasonable steps required to verify the age of an individual;

(d) the provision of reasonable assistance to children and young people to understand and communicate decisions; and

(e) the requirements to obtain consent from a person with parental responsibility for the child or young person in appropriate circumstances.

Recommendation 68–5 Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should address in their Privacy Policies how such information is managed and how the agency or organisation will determine the capacity of individuals under the age of 18.

Recommendation 68–6 Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should ensure that relevant staff receive training about issues concerning capacity, including when it is necessary to deal with third parties on behalf of those individuals.

69. Particular Privacy Issues Affecting Children and Young People

Recommendation 69–1 Schools subject to the *Privacy Act* should clarify in their Privacy Policies how the personal information of students will be handled, including when personal information:

(a) will be disclosed to, or withheld from, persons with parental responsibility and other representatives; and

(b) collected by school counsellors will be disclosed to school management, persons with parental responsibility, or others.

Recommendation 69–2 The Ministerial Council on Education, Employment, Training and Youth Affairs should consider the handling of personal information in schools, with a view to developing uniform policies across the states and territories consistent with the *Privacy Act*.

70. Third Party Representatives

Recommendation 70–1 The *Privacy Act* should be amended to include the concept of a 'nominee' and provide that an agency or organisation may establish nominee arrangements. The agency or organisation should then deal with an individual's nominee as if the nominee were the individual.

Recommendation 70–2 The *Privacy Act* should be amended to provide for nominee arrangements, which should include, at a minimum, the following elements:

(a) a nomination can be made by an individual or a substitute decision maker authorised by a federal, state or territory law;

(b) the nominee can be an individual or an entity;

(c) the nominee has a duty to act at all times in the best interests of the individual; and

(d) the nomination can be revoked by the individual, the nominee or the agency or organisation.

Recommendation 70–3 The Office of the Privacy Commissioner should develop and publish guidance for dealing with third party representatives, including in relation to:

(a) the involvement of third parties, with the consent of an individual, to assist the individual to make and communicate privacy decisions;

(b) establishing and administering nominee arrangements;

(c) identifying and dealing with issues concerning capacity; and

(d) recognising and verifying the authority of substitute decision makers authorised by a federal, state or territory law.

Recommendation 70–4 Agencies and organisations that regularly handle personal information about adults with limited or no capacity to provide consent, make a request or exercise a right under the *Privacy Act*, should ensure that relevant staff are trained adequately in relation to issues concerning capacity, and in recognising and verifying the authority of third party representatives.

Part J—Telecommunications

71. *Telecommunications Act*

Recommendation 71–1 Part 13 of the *Telecommunications Act 1997* (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.

Recommendation 71–2 The Australian Government should initiate a review to consider whether the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how these two Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and

(e) whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a public interest monitor.

Recommendation 71–3 The *Telecommunications Act 1997* (Cth) should be amended to provide that a breach of Divisions 2, 4 and 5 of Part 13 of the Act may attract a civil penalty in addition to a criminal penalty. The Australian Communications and Media Authority should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil or a criminal penalty is made.

Recommendation 71–4 The Australian Communications and Media Authority, in consultation with the Office of the Privacy Commissioner, Communications Alliance, the Telecommunications Industry Ombudsman, and other relevant stakeholders, should develop and publish guidance that addresses privacy issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping.

Recommendation 71–5 Section 117(1)(k) of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority cannot register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

Recommendation 71–6 Section 134 of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority cannot determine or vary an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

72. Exceptions to the Use and Disclosure Offences

Recommendation 72–1 Sections 280(1)(b) and 297 of the *Telecommunications Act 1997* (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.

Recommendation 72–2 The *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure of information or a document is permitted if a person has reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

Recommendation 72–3 The *Telecommunications Act 1997* (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the *Privacy Act* about an individual who is an existing customer aged 15 or over for the purpose of direct marketing only where the:

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

(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(c) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider.

Recommendation 72–4 The *Telecommunications Act 1997* (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the *Privacy Act* about an individual who is an existing customer and is under 15 years of age for the purpose of direct marketing only in the following circumstances:

(a) either the:

(i) individual has consented; or

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

(b) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider;

(c) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;

(d) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(e) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.

Recommendation 72–5 The *Telecommunications Act 1997* (Cth) should be amended to provide that in the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:

(a) comply with this requirement within a reasonable period of time; and

(b) not charge the individual for giving effect to the request.

Recommendation 72–6 A note should be inserted after s 280 of the *Telecommunications Act 1997* (Cth) cross-referencing to Chapter 4 (Access to telecommunications data) of the *Telecommunications (Interception and Access) Act 1979* (Cth).

Recommendation 72–7 Sections 287 and 300 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if:

(a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to a person's life, health or safety.

Recommendation 72–8 Section 289 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(a) the other person has consented to the use or disclosure; or

(b) the use or disclosure is made for the purpose for which the information or document came to the person's knowledge or into the person's possession (the primary purpose); or

(c) the use or disclosure is for a purpose other than the primary purpose (the secondary purpose); and

    (i) the secondary purpose is related to the primary purpose, and if the information or document is sensitive information (within the meaning of the *Privacy Act*), the secondary purpose is directly related to the primary purpose; and

    (ii) the other person would reasonably expect the person to use or disclose the information.

Recommendation 72–9 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that 'consent' means 'express or implied consent'.

Recommendation 72–10 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that use or disclosure by a person of credit reporting information is to be handled in accordance with the *Privacy Act.*

Recommendation 72–11 The *Telecommunications Act 1997* (Cth) should be amended to clarify when a use or disclosure of information or a document held on the integrated public number database is permitted.

Recommendation 72–12 Clause 3 of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (Cth) should be amended to provide that 'enforcement agency' has the same meaning as that provided for in the *Telecommunications (Interception and Access) Act 1979* (Cth).

Recommendation 72–13 Section 285 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a disclosure of an unlisted number is permitted if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.

Recommendation 72–14 The Australian Government should amend s 285(3) of the *Telecommunications Act 1997* (Cth) to provide that before the Minister specifies a kind of research for the purpose of the use or disclosure of information or a document contained in the Integrated Public Number Database, the Minister must be satisfied that the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the Integrated Public Number Database.

Recommendation 72–15 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Privacy Commissioner, as soon as practicable after becoming aware:

(a) of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of protected information; and

(b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.

Recommendation 72–16 The *Telecommunications Act 1997* (Cth) should be amended to provide that directory products that are produced from data sources other than the Integrated Public Number Database should be subject to the same rules under Part 13 of the *Telecommunications Act* as directory products which are produced from data sourced from the Integrated Public Number Database.

Recommendation 72–17 The *Telecommunications Act 1997* (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

73. Other Telecommunications Privacy Issues

Recommendation 73–1 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, in the possession of an agency, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

Recommendation 73–2 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to require the destruction of non-material content intercepted under a B-Party warrant.

Recommendation 73–3 The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the Australian Security Intelligence Organisation and enforcement agencies must destroy in a timely manner irrelevant material containing accessed telecommunications data which is no longer needed for a permitted purpose.

Recommendation 73–4 Sections 151 and 163 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide for reporting requirements relating to the use of stored communication warrants that are equivalent to the interception warrant reporting requirements under Part 2–7 and s 102 of the Act.

Recommendation 73–5 The Australian Government Attorney-General's Department should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act 1979* (Cth), that addresses:

(a) the definition of the term 'telecommunications data';

(b) when voluntary disclosure of telecommunications data to the Australian Security Intelligence Organisation and other enforcement agencies is permitted; and

(c) timeframes within which agencies should review holdings of information and destroy information.

Recommendation 73–6 The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide expressly that where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection of the agency's records relating to access to a stored communication, the Ombudsman may:

(a) require the officer to give the information to the Ombudsman and to attend a specified place in order to answer questions relevant to the inspection; and

(b) where the Ombudsman does not know the officer's identity, require the chief officer, or a person nominated by the chief officer, to answer questions relevant to the inspection.

Recommendation 73–7 The Australian Communications and Media Authority should add the Office of the Privacy Commissioner as a member of the Law Enforcement Advisory Committee.

Recommendation 73–8 The Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority should develop memorandums of understanding, addressing:

(a) the roles and functions of each of the bodies under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and *Privacy Act*;

(b) the exchange of relevant information and expertise between the bodies; and

(c) when a matter should be referred to, or received from, the bodies.

Recommendation 73–9 The document setting out the Office of the Privacy Commissioner's complaint-handling policies and procedures (see Recommendation 49–8), and its enforcement guidelines (see Recommendation 50–3) should address:

(a) the roles and functions of the Office of the Privacy Commissioner, Telecommunications Industry Ombudsman and the Australian Communications and Media Authority under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and *Privacy Act*; and

(b) when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.

Recommendation 73–10 The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should:

(a) outline the interaction between the *Privacy Act*, *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth);

(b) provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and

(c) outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act*, *Spam Act* and *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.

Recommendation 73–11 The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish educational material that addresses the:

(a) rules regulating privacy in the telecommunications industry; and

(b) various bodies that are able to deal with a telecommunications privacy complaint, and how to make a complaint to those bodies.

Part K—Protection of a Right to Personal Privacy

74. Protecting a Right to Personal Privacy

Recommendation 74–1 Federal legislation should provide for a statutory cause of action for a serious invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, a serious invasion of privacy may occur where:

(a) there has been an interference with an individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

(d) sensitive facts relating to an individual's private life have been disclosed.

Recommendation 74–2 Federal legislation should provide that, for the purpose of establishing liability under the statutory cause of action for invasion of privacy, a claimant must show that in the circumstances:

(a) there is a reasonable expectation of privacy; and

(b) the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

In determining whether an individual's privacy has been invaded for the purpose of establishing the cause of action, the court must take into account whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression).

Recommendation 74–3 Federal legislation should provide that an action for a serious invasion of privacy:

(a) may only be brought by natural persons;

(b) is actionable without proof of damage; and

(c) is restricted to intentional or reckless acts on the part of the respondent.

Recommendation 74–4 The range of defences to the statutory cause of action for a serious invasion of privacy provided for in federal legislation should be listed exhaustively. The defences should include that the:

(a) act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(b) act or conduct was required or authorised by or under law; or

(c) publication of the information was, under the law of defamation, privileged.

Recommendation 74–5 To address a serious invasion of privacy, the court should be empowered to choose the remedy that is most appropriate in the circumstances, free from the jurisdictional constraints that may apply to that remedy in the general law. For example, the court should be empowered to grant any one or more of the following:

(a) damages, including aggravated damages, but not exemplary damages;

(b) an account of profits;

(c) an injunction;

(d) an order requiring the respondent to apologise to the claimant;

(e) a correction order;

(f) an order for the delivery up and destruction of material; and

(g) a declaration.

Recommendation 74–6 Federal legislation should provide that any action at common law for invasion of a person's privacy should be abolished on enactment of these provisions.

Recommendation 74–7 The Office of the Privacy Commissioner should provide information to the public concerning the recommended statutory cause of action for a serious invasion of privacy.

Model Unified Privacy Principles (UPPs)

Contents

UPP 1. Anonymity and Pseudonymity

Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:

(a) not identifying themselves; or

(b) identifying themselves with a pseudonym.

UPP 2. Collection

2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

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

(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.

2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented;

(b) the collection is required or authorised by or under law;

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;

(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual's consent;

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(f) the collection is necessary for research and all of the following conditions are met:

(i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable;

(ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;

(iii) 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*; and

(iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or

(g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Note: Agencies and organisations that collect personal information about an individual from an individual or from someone else must comply with UPP 3.

UPP 3. Notification

3. At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

(a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;

(b) identity and contact details of the agency or organisation;

(c) rights of access to, and correction of, personal information provided by these principles;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;

(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and

(h) fact, where applicable, that the collection is required or authorised by or under law.

UPP 4. Openness

4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:

(a) sort of personal information the agency or organisation holds;

(b) purposes for which personal information is held;

(c) avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and

(e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

(a) electronically; and

(b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.

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.

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.

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.

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.

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.

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.

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).

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;

(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.

Executive Summary

Contents

Introduction to the ALRC's Privacy Inquiry

For Your Information: Australian Privacy Law and Practice represents the culmination of a 28 month inquiry into the extent to which the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia. This Inquiry was a mammoth undertaking, resulting in the three volumes of this Report, containing 74 chapters and 295 recommendations for reform.

The *Privacy Act* is itself substantially the product of an earlier ALRC inquiry—a seven year research and policy development exercise ending in 1983 with the publication of the three volume report entitled *Privacy*.[1] As discussed in Chapter 1, the enactment of privacy legislation in Australia represented partial fulfilment of Australia's international obligations under the *International Covenant on Civil and Political Rights*, which recognises a basic human right to privacy premised on the autonomy and dignity of the individual.[2] The ALRC's work not only led to domestic legislation but also strongly influenced the international development of this field. The ALRC's Chair at that time, Justice Michael Kirby, was asked to chair two key Organisation for Economic Co-operation and Development working groups in the 1980s, on privacy principles and data security.

As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. Although the ALRC often heard emphatic arguments couched in the language of rights, international instruments on human rights, and the growing international and domestic jurisprudence in this field, all recognise that privacy protection is not an absolute. Where circumstances require, the vindication of individual rights must be balanced carefully against other competing rights—and the ALRC's final recommendations in this Report endeavour to do so.

The privacy implications of developing technology were not lost on the Commission in 1983—and the ALRC was surprisingly prescient in its understanding of emerging computer power and the associated privacy concerns. However, the now ubiquitous use of personal computers, mobile phones and cameras, the internet, radio frequency identification devices, global positioning systems, surveillance cameras, smart cards, biometrics and a myriad of other technological developments—while perhaps not quite in the realm of science fiction in the 1980s—was yet to impact so comprehensively and powerfully on the daily lives of Australians.

In the new Information Age, high-powered computers and other sophisticated electronic devices are no longer the preserve of specialist technicians employed by governments and major corporations, but a basic tool utilised by virtually all Australians in almost all aspects of their lives, including for: communication with family, friends and colleagues; research and writing; entertainment and news gathering; shopping, banking and share trading; storage of important records, documents and images; and dating and social networking.

---

1 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

2 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

It became clear during the course of the current Inquiry that these rapid advances in information, communication and surveillance technologies have created a range of previously unforeseen privacy issues. At the same time, the emergence of regional political and economic blocs, such as the European Union and the Asia-Pacific Economic Cooperation group (APEC), has created pressure for the alignment of Australia's privacy protection regime with those of its key trading partners.

Further, information privacy legislation has proliferated at the state and territory level, but with no concerted effort to maintain a nationally consistent regime. Finally, the *Privacy Act* has undergone significant amendment since its enactment in 1988, resulting in an unwieldy and overly complex piece of legislation.

Extensive public engagement

The breadth of the subject matter covered in this Inquiry required the ALRC to undertake the largest community consultation program in its 33 year history. To facilitate public engagement and stakeholder participation, two issues papers, *Review of Privacy* (IP 31)[3] and *Review of Privacy: Credit Reporting Provisions* (IP 32),[4] and a three-volume Discussion Paper, *Review of Australian Privacy Law* (DP 72),[5] were released. Concise overviews of IP 31 and IP 32,[6] and DP 72,[7] also were published to reach the non-specialist audience. The ALRC organised:

- about 250 face-to-face meetings with individuals, organisations and agencies;
- major public forums in Melbourne (focusing on consumers and privacy), Sydney (focusing on business and privacy) and Coffs Harbour (focusing on health privacy and research);
- six workshops for children and young people (aimed at those aged 13–25);
- a series of roundtables with individuals, agencies and organisations on a variety of themes including: credit reporting; telecommunications; the privacy principles; children and young people; and health and research;

3 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).
4 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006).
5 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007).
6 Australian Law Reform Commission, *Reviewing Australia's Privacy Laws: Is Privacy Passé?*, Overview (2006).
7 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007).

- a highly publicised 'National Privacy Phone-In' on 1–2 June 2006, during which more than 1,300 members of the public contacted the ALRC to share their experiences, ideas and attitudes about privacy protection (see below); and

- the establishment of a 'Talking Privacy' website, designed specifically to appeal to young people.

The ALRC also actively solicited submissions, receiving 585 written submissions from a broad cross-section of individuals, organisations and agencies. The high level of public engagement with the ALRC Inquiry reflected the extent of public interest and concern about privacy protection. Community and stakeholder concerns helped direct the ALRC in developing its priorities and the ultimate reform agenda.

The scope of the *Privacy Act*

In the early stages, at least, some meetings suggested that there was a mismatch in the broader concept of privacy utilised by the general public and the way the term 'privacy' is defined in a technical legal sense in the *Privacy Act*. Experts and privacy professionals mainly concern themselves with information privacy and data security and protection. The ALRC has, in fact, recommended that the name of the Act be changed to the *Privacy and Personal Information Act*.[8]

Australians generally consider that they have a 'right to privacy'—notwithstanding the absence of a national charter of rights—and that this protection has been extended to cover the activities of the private sector as well as government agencies. Many members of the general public (and no doubt many lawyers), however, incorrectly assume that the *Privacy Act* also covers such others matters as:

- unwanted calls at home by telemarketers (now addressed by the 'Do Not Call Register');

- surveillance at work and in public places;

- spying by neighbours;

- paparazzi-type photographs; and

- police procedures, especially intrusive searches and seizures and the collection of DNA samples.

8 See Ch 5.

The National Privacy Phone-In

The ALRC kicked off the public phase of the Inquiry with a two day National Privacy Phone-In on 1–2 June 2006, which handled 1,343 responses. The results were very interesting. Nearly three-quarters of all respondents (73%) cited telemarketing as a major concern, provoking a cluster bomb of indignant questions and comments: 'It feels like a "home invasion"'; 'How did they get my number?'; 'Why do they always call at dinner time when I've got my hands full cooking and trying to settle the kids?'

This category was followed, in order of prevalence, by concerns expressed about:

- the handling of personal information by the private sector (19%);
- the handling of personal information by government (9%);
- the protection of privacy on the internet (7%);
- national identity cards and 'smart cards' (7%);
- problems accessing and correcting personal information (7%); and
- surveillance in public places (4%).

Contrary to expectations, very few comments were received about workplace surveillance (2%) or spying by neighbours (only four calls).[9]

The general lamentation: is privacy passé?

It was very evident in public forums and meetings that there is a general feeling in the community that technological advances have steadily and irreparably eroded personal privacy—'we have much less privacy than previous generations, and it will only get worse!'—and that greater efforts must be made to resist this.

When the discussion moved from the general to the specific, however, there was evident a countervailing appreciation of the parallel benefits of modern information and communication technology, with praise for the ease, convenience and empowering qualities of email, mobile phones, e-commerce, digital photography, the internet and so on.

---

9 Callers were able to nominate more than one concern, which is reflected in the statistics. Further, the nature of the comments may have been influenced by a number of media stories about the Phone-In, which focused on telemarketing as a possible concern.

People also expressed a high degree of willingness to trade off privacy interests (or at least to understand the potential compromise) to meet concerns about law and order at the local level—for example, accepting the use of surveillance cameras in public places—or about national security more generally.

Similarly, the ALRC found—despite the frequent use of the absolutist language of 'rights'—that there is general community appreciation for the need to strike a common sense balance between privacy interests and practical concerns in a range of areas. For example, while personal health information is regarded as 'sensitive' and deserving of the highest level of protections, individuals understand that a premium may be placed on prompt access to, and disclosure of, such information in the case of a medical emergency.

An emerging generation gap?

During the course of this Inquiry, the ALRC explored whether there is an emerging generation gap in basic attitudes to privacy. That is, do young people have such a fundamentally different approach to privacy that this should be recognised (or at least anticipated) by law?

It does appear that young people are more comfortable than their parents, and certainly their grandparents, in sharing personal information, photos and other material on social networking websites. The question is whether this represents the beginnings of an enduring cultural shift, or simply the eternal recklessness of youth, played out in a new medium and utilising new technology. Put another way, will today's teenagers be horrified in a decade's time when prospective employers—and prospective partners and in-laws—can easily 'google up' intimate and potentially embarrassing images and information?

As mentioned above, the ALRC went to considerable effort to consult directly with children and young people—and found that, even though there is an increased willingness to share information on websites like MySpace and Facebook, nevertheless there remains a strong desire to retain control over access to, and distribution of, this personal information. Some young people were quite savvy about how to achieve this. Many others, however, appeared to be unaware of the privacy policies of the social networking sites they frequented, and unfortunately naïve about the degree of control they can exercise in practice. Further, many young people were unaware of the extent to which information—for example, photographs—deleted from their profile remain on the internet; either as a result of downloading onto other sites or archiving.

While children and young people normally can seek guidance about moral and ethical standards of behaviour at home, at school or at their place of worship, they may find themselves pretty much on their own when operating at the cutting edge of technology.

The ALRC found, however, that there was little appetite for more law or formal regulation in this area. The consistent advice received was that much more education is

needed for children and young people—and the adults in their lives—about how to operate properly and safely in this new electronic environment. Some excellent guidance already is being published by industry bodies, and the ALRC recommends that this effort intensify and also involve the Office of the Privacy Commissioner (OPC).

Complexity and confusion

Businesses—not surprisingly—were concerned mainly with the overly complex and confusing web of privacy laws in Australia, citing the overlapping federal, state and territory laws; the separate privacy principles for government agencies (the Information Privacy Principles (IPPs)) and private sector organisations (the National Privacy Principles (NPPs)), and other relevant laws, including those covering the privacy of health information. This makes it very difficult—and expensive—for even the best-intentioned business to comply.

These concerns were expressed consistently and strongly in submissions and consultations throughout the Inquiry—making it clear to the ALRC that simplification and harmonisation of the law had to be one of the principal aims and outcomes of this Inquiry.

Enforcing compliance

The ALRC often heard concerns that the *Privacy Act* is a 'toothless tiger', lacking adequate enforcement mechanisms and sufficient sanctions to ensure compliance. Whether this is a real or a perceived problem, the ALRC takes very seriously the need to improve the regulatory scheme and to increase community confidence in the level of compliance with the requirements of the Act.

The ALRC actively sought and received community and stakeholder comment in this area, and makes a number of recommendations (see below) aimed at addressing: the structure, role and powers of the OPC; improvements to the complaint-handling process; the Privacy Commissioner's ability to require a Privacy Impact Assessment for a new project or development that may have a significant impact on the handling of personal information; the Privacy Commissioner's powers to conduct audits, monitor compliance, and to issue notices to comply where required; greater powers for the OPC to spur the development of context or industry-specific privacy codes, to flesh out the general privacy principles; and the ability of the OPC to pursue civil penalties in a federal court, where there is a serious or repeated misuse of an individual's personal information.

The BOTPA excuse: 'Because of the *Privacy Act*'

Interestingly, a range of callers to the National Privacy Phone-In argued that sometimes there may be '*too much* privacy'—or rather that 'privacy' is all too often trotted out as an excuse for inaction or non-cooperation. Among privacy professionals,

this has become known as the 'BOTPA' excuse, since people are told that their reasonable requests cannot be accommodated 'because of the *Privacy Act*'. For example, the ALRC heard complaints from people who, 'because of the *Privacy Act*', were unable to:

- access or correct their own personal information held on a government or corporate database;
- assist an elderly relative or neighbour with their banking, or in dealing with a public utility or government agency—even where that person had written authorisation or held a valid power of attorney; and
- urge their church congregation to pray for a named individual who was unwell and in hospital.

Key recommendations

Having listened carefully to the views, concerns and feedback expressed during the extensive community consultation exercise, and conducted its own research and deliberations, the ALRC has developed and presents in this Report a large set of policy recommendations for improving privacy protection in Australia. Some of the key recommendations are explained below.

The *Privacy Act* and privacy principles

The ALRC recommends that the *Privacy Act* be redrafted and restructured to achieve significantly greater consistency, clarity and simplicity.

A key element of this reform would be a rationalisation of the privacy principles, which address the handling of personal information by agencies and organisations covered by the *Privacy Act*. There are currently two separate sets of privacy principles contained in the *Privacy Act*:

- the IPPs, which apply to the handling of personal information by Commonwealth and ACT public sector agencies; and
- the NPPs, which apply to many private sector organisations (including not-for-profit organisations, but not most small businesses).

The ALRC recommends that these be unified into a single set of privacy principles, covering information handling in both the public and private sectors. For the purposes of this Inquiry, these principles are referred to as the model Unified Privacy Principles (UPPs),[10] and cover the following areas:

---

10 The ALRC anticipates that the principles may be renamed when the *Privacy Act* is redrafted.

- Anonymity and Pseudonymity;
- Collection;
- Notification;
- Openness;
- Use and Disclosure;
- Direct Marketing;
- Data Quality;
- Data Security;
- Access and Correction;
- Identifiers; and
- Cross-Border Data Flows.

The ALRC sees 'principles-based regulation' as the primary method of regulating information privacy in Australia. It is important to note, however, that the ALRC does not recommend the adoption of a pure form of principles-based regulation. In order to achieve the necessary policy outcomes, the ALRC adopts a pragmatic approach to the formulation of the model UPPs and its recommended regulatory model. For example, in some circumstances, the UPPs will need to be supplemented with more specific rules (promulgated in regulations or other legislative instruments), in order to accommodate the particular needs and circumstances of different industries.

The ALRC recommends a basic restructure of privacy regulation to follow this three-tiered approach:

- high-level principles of general application, provided in a streamlined *Privacy Act*;
- regulations and industry codes, detailing the handling of personal information in certain specified contexts, such as health and research, and credit reporting; and
- guidance issued by the Privacy Commissioner (and other relevant regulators), dealing with operational matters and explaining to end users what is expected in various circumstances, as well as providing basic advice and education.

National consistency

The Australian Government is not alone in seeking to regulate the handling of personal information in Australia—every state and territory also has legislation or administrative guidelines in this area. This creates confusion for individual consumers, who cannot always be expected to know whether an agency is a federal, state or territory body or, as a result, where to go for guidance on which privacy laws apply or where to take concerns and complaints.

In addition to general information privacy legislation, New South Wales, Victoria and the ACT also have specific laws on the handling of health information, which apply to state public sector agencies and private sector organisations. This creates uncertainty for health service providers and consumers, because private health services (including not-for-profit health services) may be covered by the federal *Privacy Act*, as well as by specific state or territory health privacy legislation. Health services that operate across state and territory borders may have to comply with multiple laws, each with different requirements.

There is little doubt that there would be great benefits across the board from adopting a common approach to privacy protection in all Australian jurisdictions. To achieve greater consistency, the ALRC recommends that the *Privacy Act* should apply to the federal public sector and the private sector—to the exclusion of state and territory laws dealing specifically with the privacy of personal information, including personal health information, handled by organisations.

The Commonwealth, state and territory governments should establish an intergovernmental cooperative scheme, under which the states and territories will agree to enact legislation to regulate the handling of personal information in each state's and territory's public sector by adopting the key elements of the *Privacy Act*—such as the same set of privacy principles, important definitions, data breach notification schemes and other key provisions.

The approach recommended by the ALRC would make it far easier for individuals to understand the general rules that apply to personal information—regardless of whether it is being handled by a private organisation, a federal agency, or a state or territory agency—and would ease the compliance burden significantly and reduce costs for business.

Key definitions

Important definitions in the *Privacy Act*—such as the definition of 'personal information', 'sensitive information' and 'record'—should be updated to deal with new technologies and new methods of collecting and storing personal information.

The definition of 'personal information' should be amended to bring it more into line with other jurisdictions and international instruments.

Sensitive information—which is given a higher level of protection than other personal information under the NPPs—is defined in the *Privacy Act* to include information about particular types of personal characteristics, including racial or ethnic origins, political opinions, religious beliefs and sexual orientation. The ALRC heard concerns that biometric technologies—such as facial and gait recognition systems—may be used without an individual's knowledge or consent, and could reveal other sensitive personal information, such as information about a person's health or racial or ethnic origins. To address this concern, the ALRC recommends that the definition of 'sensitive information' be amended to include certain types of biometric information.

The definition of 'record' should be amended to ensure greater consistency with other legislation, and to clarify that a record may be stored in electronic or other formats.

Rationalisation and clarification of exemptions

The current fragmentation and complexity of privacy protection in Australia is exacerbated by the number of exemptions from, and exceptions to, the requirements of the *Privacy Act*. Complete exemptions from the coverage of the Act should be permitted only where there is a compelling policy basis for so doing. The ALRC recommends that the number of exemptions be reduced—in particular, the existing exemptions for small business, employee records and registered political parties should be removed.

The small business exemption

When the provisions of the *Privacy Act* were extended to cover the private sector in December 2000, an exemption was granted to small businesses (including not-for-profit organisations) with an annual turnover of $3 million or less.[11] The exemption was explained, at that time, by the desire to achieve widespread acceptance for privacy regulation from the private sector, and a reluctance to impose additional compliance burdens on small businesses.

No other comparable jurisdiction in the world exempts small businesses from the general privacy law—and the European Union specifically has cited this unusual exemption as a major obstacle to Australia being granted 'adequacy' status under the European Union *Directive on the Protection of Individuals with Regard to the*

11 There are some exceptions to this general rule—for example, small health service providers handling sensitive personal information.

Processing of Personal Data and on the Free Movement of Such Data (the EU Directive).[12]

The business community argued strongly for the retention of the exemption, primarily on the basis of the cost of compliance. However, almost all other stakeholders supported removal of the exemption arguing that there is no compelling justification for a blanket exemption for small businesses, as consumers have the right to expect that their personal information will be treated in accordance with the privacy principles.

The ALRC recommends that this exemption be removed. This would bring Australian privacy laws into line with laws in similar jurisdictions, such as the United Kingdom (UK), Canada and New Zealand, and could facilitate trade by helping to ensure that Australia's privacy laws are recognised as 'adequate' by the European Union. The removal of the small business exemption would have the additional benefits of simplifying the law and removing uncertainty for many small businesses that have difficulty establishing whether they are required to comply with the *Privacy Act*.

The ALRC appreciates that the removal of the small business exemption will have cost implications for the sector—although nowhere near as great as is sometimes predicted.[13] An independent research study commissioned by the ALRC indicated that a lower proportion of organisations will be affected—since not all small businesses collect personal information from customers—and the costs should be considerably more modest—about $225 in start-up costs and $301 per year thereafter for each small business—than the predicted $842 and $924 per year respectively cited in the Office of Small Business costing.[14] Further, the ALRC is confident that additional savings will be achieved by the substantial simplification and harmonisation of privacy laws recommended in this Report.

Nevertheless, the ALRC remains attentive to the economic concerns of small business owners, and recommends a number of other initiatives aimed at supporting small businesses and minimising the compliance burden. Before the exemption is removed, the OPC should provide support to small businesses to assist them in understanding and fulfilling their obligations under the *Privacy Act*. This should include a national hotline for small businesses, education materials and templates to assist in preparing privacy policies.

---

12 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).

13 See Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007), as discussed in Ch 39.

14 Ibid.

Employee records exemption

While public sector agencies are required to treat employee records in accordance with the *Privacy Act*, private organisations generally are exempt in relation to current and past employees (with some limited exceptions). There seems little justification in principle for the differential approach—which does not feature in the law of comparable jurisdictions.

The ALRC recommends that this exemption be removed. This would create consistent rules for personal information about employees, regardless of whether they are public or private sector employees.

The ALRC acknowledges that there may be circumstances in which it is undesirable to allow employees to have access to all of the information contained in their files—such as referees' reports and other similarly confidential material. It would be much better practice to deal with such exceptions on the basis of the general law of confidentiality, however, rather than wholly exempting private sector employers from the normal requirements of the *Privacy Act*.

The 'Access and Correction' principle in the model UPPs permits an organisation or agency to deny a request for access to personal information in certain circumstances. For example, where access by an employee to evaluative material, such as references, would lead to a breach of confidence by the organisation, the organisation would be able to deny access on the basis that it is required or authorised by or under law.

Political parties, acts and practices exemption

Registered political parties are specifically excluded from the definition of 'organisation' and, therefore, are exempt from the operation of *Privacy Act*. In addition, political acts and practices of certain organisations—including political representatives, volunteers for political parties, and contractors and subcontractors of political parties and political representatives—are exempt from the Act.

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, and developing policies and advertising strategies. Arguments supporting the exemption generally are based on the importance of freedom of political communication to Australia's robust democratic process. The position varies in other comparable countries—political parties are similarly exempt in the United States (US) and Canada, but compliance with privacy laws is required in the UK, New Zealand and Hong Kong.

There was considerable support in the general community, however, for removing the exemption. Some stakeholders argued that the preferential treatment accorded

registered political parties undermines public trust in the political process. Others were concerned that because of the exemption: political parties can collect information about constituents from third parties that could be inaccurate; individuals do not know what information has been collected by the parties; and have no right of access to, or correction of, personal information in electoral databases.

Journalism exemption

The acts and practices of a media organisation in the course of journalism are exempt from the operation of the *Privacy Act* where the organisation has publicly committed to observe standards that deal with privacy. This exemption reflects the balancing of competing rights, discussed above, placing a premium on protecting freedom of expression and the importance of the free flow of information to the maintenance of a healthy democracy.

No serious case was presented for the abolition of this exemption. There were some calls for refining the terms used to define it because of the difficulties associated with distinguishing journalism from commercial and other activities (especially in the convergent electronic environment).

The ALRC recommends that the scope of this exemption be clarified, by inserting a definition of 'journalism'—not currently defined in the Act. The ALRC also recommends that for the exemption to apply to an organisation, the standards to which the organisation is committed must *adequately* deal with privacy.

Improved complaint handling

The ALRC recommends the streamlining of procedures for handling complaints about alleged privacy breaches. The Privacy Commissioner should have the power to decline to investigate a complaint if, for example, the complaint is being handled by an appropriate external dispute resolution scheme.[15] Further, both complainants and respondents should have the power to require that the complaint be resolved by determination if, in the opinion of the Privacy Commissioner, all reasonable attempts to settle the complaint have failed.

Where the Privacy Commissioner determines that an agency or organisation has engaged in conduct constituting an interference with the privacy of an individual, the Commissioner should have the power to issue a notice prescribing that an agency or organisation must take specified action within a specified period, for the purpose of ensuring compliance with the *Privacy Act*. The Privacy Commissioner also should

15 The term 'external dispute resolution' (EDR) is used in this Report 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. The term includes, but is not limited to, EDR conducted by EDR schemes approved by the Australian Securities and Investments Commission: see *Corporations Act 2001* (Cth) ss 912A(2)(b), 1017G(2)(b).

have the power to commence proceedings in the Federal Court of Australia or the Federal Magistrates Court for an order enforcing the notice.

Stronger penalties

There are currently no civil penalties available for serious contraventions of the Act, and only limited (and rarely used) criminal penalties for credit reporting and tax file number offences. The ALRC recommends that the penalty regime be strengthened by allowing the Privacy Commissioner to seek a civil penalty in the federal courts where there is a serious or repeated interference with the privacy of an individual.

The structure and role of the OPC

The ALRC recommends that the OPC be renamed the Australian Privacy Commission. The *Privacy Act* also should be amended to provide for the appointment of one or more Deputy Privacy Commissioners, with the power to exercise all the powers, duties and functions of the Privacy Commissioner. This would allow the agency to expand in response to technological developments and evolving public interest in privacy. It also would allow for greater collegiate decision making, encouraging greater accountability and transparency.

Further, the *Privacy Act* should be amended to increase the powers of the Privacy Commissioner, to include the power to:

- direct an agency to provide a 'Privacy Impact Assessment' in relation to a new project or development that may have a significant impact on the handling of personal information; and

- conduct 'Privacy Performance Assessments' of the records of personal information maintained by organisations.

Data breach notification

Under existing law, agencies and organisations are not required by the IPPs or NPPs to notify individuals when their personal information has been compromised. The ALRC's attention was directed to the strong growth internationally of requirements to notify individuals where there has been unauthorised access to their personal information. For example, about 40 American states now have data breach notification schemes, contained in legislation or administrative arrangements.

It was suggested in many meetings and submissions that a data breach notification scheme was needed in Australia, with a strong preference for a national approach overseen by the OPC. People are now very aware of the nefarious activities of computer hackers and the widespread existence of 'malware', and there are regular news reports of laptops containing sensitive personal information being lost and other personal records accidentally being exposed or illicitly accessed. Particularly given the

increasing fear of identity theft and fraud, proponents argue that individuals have a right to be informed when the security and privacy of their personal information have been compromised.

In terms of regulatory theory, there are good justifications for a national data breach notification scheme, including that:

- under-reporting of breaches is highly likely, absent any express requirement;
- this would provide strong market incentives to secure databases in compliance with the 'Data Security' principle;
- this would promote greater transparency and accountability around information-handling practices;
- notification gives individuals the information and opportunity to protect themselves against fraud and identity theft; and
- the development of a national model is preferable to a proliferation of differing state and territory schemes—as has happened in the US.

On the other side, the ALRC heard concerns from agencies and organisations about: the costs associated with notification, particularly where the relative risk of harm to individuals is small; the dangers of 'notification fatigue'; and a desire not to scare people away from e-commerce and other online services.

While recognising the sense and inevitability of some form of data breach notification scheme in Australia, agencies and organisations argued for one that adopted a reasonable balance, triggered only where there is a real risk of significant harm to individuals, and without unduly prescriptive or costly mechanics of notification (in terms of form, content, timing and method of distribution).

The ALRC recommends that the *Privacy Act* be amended to require an agency or organisation to notify the Privacy Commissioner and affected individuals when a data breach has occurred that may give rise to serious harm to any affected individual.

Decision making by children and young people

Issues relating to the privacy of children and young people often were raised in meetings and submissions. There is evident uncertainty in the community about the extent to which young people have the capacity to make decisions for themselves about the collection, use and disclosure of their personal information.

The *Privacy Act* is currently silent about the age at which children and young people should be able to make decisions about their own personal information.

Although arising in a range of circumstances, the biggest concern raised in consultations related to the use and disclosure of health and medical information—for example, whether young people (under the age of 18) could ask their family doctor not to disclose their personal health information to parents; and conversely whether parents could seek access to their teenage children's health records. (Note that consent to medical treatment—as opposed to the collection, use and disclosure of health information—is *not* a matter regulated by the *Privacy Act* and therefore is not considered in this Report).

Research on child development and adolescent brain development suggests that the capacity to make decisions evolves through childhood and adolescence, and is dependent on individual characteristics and the particular decision concerned. As in other inquiries in which similar issues have arisen—including the ALRC's reports on the rights of the child[16] and uniform evidence laws[17]—the ALRC has sought to shift the debate away from the imposition of a fixed age for decision making, towards an assessment (where possible) of the young person's capacity to make decisions about personal information.

For this reason, the ALRC has not recommended that the *Privacy Act* set a fixed age at which children and young people are deemed to be able to make their own decisions. Instead, the ALRC recommends that where it is practicable to make an assessment about capacity, such an assessment should be undertaken.

The ALRC recognises, however, that there are some situations in which it is difficult for an agency or organisation to make an assessment about decision-making capacity. The ALRC recommends that, where such an assessment is not reasonable and practicable, an individual aged 15 years or over should be presumed to be capable of giving consent, making a request or exercising a right of access concerning his or her personal information. This is consistent with the age at which a young person is able to obtain a separate Medicare card without parental consent. Individuals under the age of 15 must have a person with parental responsibility make the decision on their behalf, where it is not possible to assess decision-making capacity.

Nominee arrangements

The ALRC also heard many stories from people who were frustrated in their efforts to assist adult relatives and friends who are unable to act for themselves due to some temporary or permanent incapacity. It appears that in many of these cases the problems were occasioned by an incorrect or inflexible application of the *Privacy Act*. Similarly, some individuals may have the capacity to make their own decisions about privacy, but

16 Australian Law Reform Commission, *Seen and Heard: Priority for Children in the Legal Process* (ALRC 84, 1997).

17 Australian Law Reform Commission, *Uniform Evidence Laws* (ALRC 102, 2005).

need assistance in dealing with agencies or organisations—for example, due to limited mobility or language difficulties.

The ALRC makes a number of recommendations in this Report aimed at clarifying the legal position, to facilitate authorised persons rendering assistance in such cases—and minimising the 'BOTPA' problem. First, the *Privacy Act* should be amended to include the concept of a 'nominee', appointed by an individual, to make decisions and requests in relation to the individual's personal information. Once established, the agency or organisation should deal with an individual's nominee, to the extent provided in the nominee arrangement, as if the nominee were the individual concerned.

Further, the ALRC recommends that the OPC publish guidance for agencies and organisations on the proper involvement of third parties in communicating and making privacy decisions for those requiring assistance.

More comprehensive credit reporting

Little comment was aroused from the general public about the issue of credit reporting—but there was a very high level of engagement with the Inquiry in this area from credit providers and credit reporting organisations on the one hand, and privacy advocates and consumer groups on the other.

Perhaps unbeknown to most members of the community, Part IIIA of the *Privacy Act* regulates the system of credit reporting, allowing information about an individual's credit worthiness to be collected and disclosed to credit providers, such as banks, finance companies, mortgage companies, and mobile phone service providers. This information is collected by a small number of specialist credit reporting companies from credit providers and publicly available records.

The Australian regime is currently considerably more restrictive than in most comparable countries in relation to the types of information that may be collected and disclosed. Put simply, credit files are limited to information that might detract from an individual's credit worthiness, or so-called 'negative information'.

Credit providers and credit reporting bodies argued strongly for a wider range of information—such as current credit balances and loan repayment histories—to be collected and disclosed in reports to lenders, on the basis that such information is required for credit providers to make good decisions about an applicant's ability to service the requested level of debt. The industry was very active in supplying the ALRC with studies, surveys, reports and economic modelling suggesting that an increase in the 'positive' information available to lenders would facilitate better risk management practices, which in turn would open up the field to greater competition and drive down the cost of credit—especially for low risk and responsible borrowers.

At the same time, privacy and consumer advocates (and the Privacy Commissioner) argued strongly that allowing large amounts of sensitive information on the financial position and credit behaviour of individuals to be collected in private databases would pose greater risks to security and privacy—and, indeed, a number of previous inquiries into this area in Australia have failed to recommend any significant changes to the system.

The Australian credit industry itself is divided about how much more personal information is required—or, perhaps, is realistically obtainable given the opposition. Some credit providers pushed for 'comprehensive credit reporting' in keeping with practice in the US and the UK. During the life of the Inquiry, however, a consensus seemed to form around a more moderate approach—a system of 'more comprehensive credit reporting' that would add some additional categories of 'positive' information to an individual's credit information file, without going as far as the US or UK systems.

The ALRC recommends that the credit reporting provisions of the *Privacy Act* (Part IIIA) be repealed and credit reporting regulated under the general provisions of the Act (including the new credit reporting regulations), and the model UPPs.

Further, there should be some expansion of the categories of personal information that can be included in credit reporting information held by credit reporting agencies ('more comprehensive credit reporting'), to include: the type of each current credit account opened (eg, mortgage, credit card, personal loan); the date on which each current credit account was opened; the credit limit of each current account; and the date on which each credit account was closed.

The ALRC recognises that there are strong arguments in favour of also including an individual's repayment history in the categories of personal information that may be held by credit reporting agencies. The most compelling argument in favour of inclusion is that this will encourage more responsible lending practices. Some have questioned, however, whether more responsible lending will result from this change, in the absence of new obligations on credit providers.[18]

Consequently, the ALRC recommends that the Australian Government only amend the *Privacy Act* to allow credit reporting to include information about an individual's repayment history after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

---

18 That good risk management and responsible lending practices are not inevitable outcomes of comprehensive credit reporting is borne out by the major 'sub-prime loan' crisis in the US and the UK—where lenders have access to comprehensive information about prospective borrowers, but nevertheless made conspicuously poor decisions for years, based on the pursuit of market share and short-term incentives.

The ALRC's other recommendations for reform of credit reporting requirements include that credit providers should be prohibited from using or disclosing credit reporting information for the purposes of direct marketing, and may list overdue payment information only where the credit provider is a member of an external dispute resolution scheme approved by the Privacy Commissioner.

Privacy and telecommunications

While telecommunications legislation provides for unlisted or silent telephone numbers, it does not prohibit the charging of a fee to an individual who requests that his or her number not be listed in a public directory. The charging of a fee limits the ability of individuals—particularly those on low incomes—to control the use and disclosure of their personal information. The ALRC recommends that the charging of a fee for an unlisted (silent) number on a public number directory be prohibited by law.

A number of stakeholders told the ALRC that Part 13 of the *Telecommunications Act 1997* (Cth)—which deals with the use and disclosure of personal information in the telecommunications industry—is confusing and could be improved. The ALRC recommends that this Part of the *Telecommunications Act* be redrafted to achieve greater logical consistency, simplicity and clarity.

Health information

Overlap and complexity

There is a strong view in the community—reflected in the *Privacy Act*—that personal health information is 'sensitive information', requiring a high level of protection. A very significant concern in this area is the complexity, fragmentation and inconsistency of legislation and regulation relating to health privacy. As mentioned above, complexity is a serious concern across the whole field of privacy protection, but is perhaps most compelling in the regulation of health information.

Apart from the general recommendations made to promote national consistency,[19] the ALRC recommends that new *Privacy (Health Information) Regulations* be drafted, containing those requirements that are different or more specific than provided for in the model UPPs. Further, an intergovernmental agreement should be developed to ensure that the privacy regulation of health information (including relevant definitions) is harmonised across all Australian jurisdictions.[20]

Access to personal health information

The ALRC also heard many people express frustration about difficulties experienced in accessing or controlling their own health information—for example, patients who wished to have their medical records transferred to another doctor, whether for reasons of convenience or dissatisfaction with the services provided. Similarly, the ALRC

19 See Ch 3.
20 See Ch 3.

heard that there was a particular problem in gaining access to files where a health service closed (eg, where the doctor retired or passed away) or was taken over by another provider. The ALRC recommends that, in these circumstances, patients should be contacted and informed of the proposed arrangements for the transfer or storage of their medical records.[21]

Electronic health records

The Inquiry coincided with a number of major initiatives to develop an electronic record-keeping schemes by doctors and hospitals, aimed at providing better quality and safer health care—including the creation of a national shared electronic health information system, in which a summary of personal information is stored on a central database that can be accessed by a range of health service providers. For example, under this scheme, where an individual normally resident in New South Wales falls seriously ill or is involved in an accident in Queensland and is unable to communicate, local health authorities would be able to determine quickly whether the person suffered from any chronic medical conditions or allergies, and what medicines he or she had been prescribed.

Although there was widespread recognition of the obvious benefits of such a scheme, concerns were expressed about the architecture, security and privacy safeguards built into the system. The ALRC recommends that if national Unique Healthcare Identifiers or a national Shared Electronic Health Records scheme go forward, they should be established under specific enabling legislation, which addresses the key information privacy issues, including: the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems; the eligibility criteria, rights and requirements for participation in such schemes by health consumers and health service providers, including consent requirements; permitted and prohibited uses and linkages of the personal information held in the systems; safeguards in relation to the use of UHIs; and sanctions for misuse.[22]

Greater facilitation of research

The *Privacy Act* allows researchers to obtain and use personal information for health or medical research, without the consent of the individuals concerned, where approved by a Human Research Ethics Committee.

The ALRC heard many concerns, however, from researchers in the health and medical field—as well as social scientists, criminologists and others—that an overly cautious approach to the application of the *Privacy Act* was inhibiting the conduct of research, even where the threat to individual privacy was limited or non-existent and the

21 See Ch 63.
22 See Ch 61.

potential value of the research was very high. For example, epidemiological research can play a very valuable role in planning and promoting public health campaigns and in allocating scarce resources. In such cases, researchers are not concerned with the identity or information of individuals within the sample, but rather are seeking to identify broad trends and patterns in the population.

The ALRC also recognises that there are other forms of research that provide benefits to the community that require access to personal information in situations where it is difficult to obtain consent—such as research on child protection or factors associated with criminal behaviour.

The ALRC recommends that the research exception to the 'Collection' and 'Use and Disclosure' principles in the model UPPs allow information to be collected, used and disclosed for research purposes—including in areas other than health and medical research—where a number of conditions are met, including approval by a Human Research Ethics Committee.[23]

Cross-Border data flows

The ALRC quickly learned that an effective regulatory strategy cannot be developed under an outdated paradigm that assumes information can be contained within local or national borders, or that cross-border data flows are exceptional. It is now commonplace for major companies in Australia dealing with great volumes of personal information—including banks, insurance companies, credit card companies and others—to conduct their 'back office' processing of data overseas (often in Asia).

Indeed, privacy experts suggest it may be anachronistic even to talk about data 'flowing'—as if it there is a series of distinct, point-to-point transfers, when in fact this information is distributed across a number of databases and data centres in a number of countries, and is accessible globally by electronic means.

Similarly, individuals increasingly purchase goods and services over the internet on sites based overseas, paying with a credit card. A seemingly simple purchase of a book or DVD from a popular website, such as Amazon.com, actually may involve personal information flowing across many jurisdictions, with identity and credit verification, data processing, stock checking and shipping all handled in different countries.

Although now far more common than in previous decades, the concept of cross-border data flows is not something new. In Australia, the *Privacy Act* already deals with this phenomenon in NPP 9, which is modelled on arts 25–26 of the EU Directive.

---

23 See Chs 65, 66.

In both the ALRC's previous work on genetic privacy and discrimination (2001–2003)[24] and the current Privacy Inquiry, the ALRC consistently heard serious concerns expressed by members of the general public about their personal information being sent or held overseas without their express consent. In most cases, this unease did not reflect a specific critique of the adequacy or otherwise of the relevant privacy regime overseas—people simply do not know the position. Rather, it appears that this is a visceral reaction and an existential anxiety—a general feeling by people that they are losing control over something deeply personal, with little ability to do anything about it, and few remedies if things go badly wrong overseas.

For their part, however, business organisations told the ALRC they want to continue to be able to choose the most effective and efficient means of storing and processing customer data—and often this means doing so overseas. Indeed, businesses wish to develop these practices further, without the time, trouble and cost of seeking customer consent to what they regard as routine cross-border data flows. For business—and for governments promoting the economic benefits of efficient information handling and increasing access to global markets for trade and labour—the premium is on providing a framework to facilitate cross-border data flows, while providing individuals with a level of assurance that this will not compromise the security or privacy of their personal information.

During the course of this Inquiry, the Australian Government played a leading role in promoting the establishment of an effective regional privacy protection regime through its work with the APEC group. As evidenced by the ALRC's participation in meetings, the APEC Privacy Framework is an important opportunity to develop a distinctive approach in our region; one that is neither as reliant upon the private sector as the American regime, nor as heavily dominated by the bureaucracy as the European regime.

APEC can and should carve out a happy medium in this area, recognising the critical role that governments must play in regulating markets, but having due regard to ease and cost of compliance for business. While easy enough to articulate, developing a common approach will be no easy matter in practice, given the diversity among APEC members in cultural, political and economic terms. Achieving total uniformity, however, is not a precondition to cooperation—ultimately what is needed is a regime that Australia and other members can be sure will deliver high standards, consistency and accountability.

---

24 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

While NPP 9 provides some protection for personal information transferred to another country by an organisation, it does not apply to government agencies; and a number of stakeholders suggested that it does not provide an adequate level of protection.

The ALRC recommends that the model UPPs include a 'Cross-Border Data Flows' principle. Under this principle an agency or organisation that transfers personal information about an individual outside Australia would remain accountable for that information, unless:

- the agency or organisation reasonably believes that the recipient or the information is subject to a law, binding scheme or contract that effectively protects the personal information in a manner that is substantially similar to the UPPs;

- the individual consents to the transfer, after being advised that the agency or organisation will no longer be accountable for personal information transferred if consent is provided; or

- the agency or organisation is required or authorised by or under law to transfer the personal information.

Statutory cause of action for a serious invasion of privacy

Jurisdictions in the US and Canada have legislated for a tort of invasion of privacy since the 1970s. While the courts in the UK do not recognise a tort by that name, the equitable action for breach of confidence has been used in practice to address the misuse of personal information, and the New Zealand courts also have recognised the existence of a common law tort of privacy.

In Australia, no jurisdiction has enshrined in legislation a cause of action for invasion of privacy. The door to the development of such an action at common law, however, was left open in 2001 by the High Court's decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*.[25] Since that time, lower court decisions in Queensland (2003) and Victoria (2007) have held that such a cause of action does indeed form part of the common law of Australia.

There was spirited debate during the Inquiry about the merits of legislating in Australia for a statutory cause of action for invasion of privacy. It is fair to say that media proprietors and most organisations are implacably opposed to the development of this cause of action—arguing that it would hinder investigative journalism and potentially infringe freedom of expression. Generally left unsaid is that photos and stories about the private lives of celebrities amount to big business, and poor practice would leave media organisations exposed to liability for damages.

---

25 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

There was strong support for the development of a cause of action in the rest of the community, including among human rights and public interest organisations that generally are among the strongest advocates for freedom of speech—indicating again that this is an area requiring a careful balancing of important competing interests, rather than a blunt assertion of the rights of one sector. There is little doubt that advances in information and communication technology have heightened concerns about the potential for serious invasions of an individual's right to privacy.

Although the activities of assertive 'paparazzi' photographers feature in any conversation, most of the concerns expressed to the ALRC related more to the private sphere than to the mainstream media—and related to ordinary citizens rather than celebrities. For example, the ALRC heard stories of (or fears about) photographic images captured in toilets or dressing rooms via small digital cameras or phones, and then shown to others or posted on internet sites. There also were concerns about poor security and privacy practices—whether negligent or malicious—exposing sensitive personal information, such as medical or financial records, to unauthorised persons.

While the ALRC considers elsewhere (see above) a number of strategies for improving compliance—and penalising non-compliance—with the requirements of the *Privacy Act*, these do not provide a remedy directly to those individuals who have been harmed in the process. Further, the *Privacy Act* deals only with information privacy.

The ALRC was moved by the calls for the creation of a statutory cause of action for cases involving a serious invasion of privacy. Recognising the need to accommodate legitimate journalistic and artistic activities and uphold the right to freedom of expression, the bar must be set high and the cause of action limited to egregious circumstances.[26]

The ALRC recommends that federal legislation provide for a statutory cause of action for a serious invasion of privacy, in circumstances including where:

- there has been an interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private communication has been interfered with; or
- sensitive facts about an individual's private life have been disclosed.

26 See Ch 74.

The cause of action should apply only where the individual had a reasonable expectation of privacy; and the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

In addition, the court would be required to consider whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest in informing the public about matters of public concern and the interest in allowing freedom of expression).

Courts should be empowered to offer a range of tailored remedies for such breaches, including the award of aggravated (but not exemplary) damages, as well as injunctions, declarations and orders for apologies and corrections.

Examples of the sort of matters intended to fall within the ALRC's recommended statutory cause of action for serious invasion of privacy include the following:

- After the break-up of their relationship, Mr A sends copies of a DVD of himself and his former girlfriend (B) engaged in sexual activity to Ms B's parents, friends, neighbours and employer;

- Mr C sets up a tiny hidden camera in the women's toilet at his workplace, capturing images of his colleagues that he downloads to his own computer and transmits to a website hosted overseas, which features similar images; and

- Ms D works in a hospital and obtains access to the medical records of a famous sportsman, who is being treated for drug addiction. D makes a copy of the file and sells it to a newspaper, which publishes the information in a front page story.

Further reviews and studies

Given the breadth of this Report, and the far-reaching impact of a number of the recommendations, it will take some time to ascertain the effect of the recommended reforms. Consequently, the ALRC also recommends that the Australian Government initiate a review in five years from the commencement of:

- the amended *Privacy Act*, to consider whether the intergovernmental cooperative scheme recommended in this Report has been effective in achieving national consistency. If the review concludes that national consistency has not been achieved, the Australian Parliament should consider whether it should exercise its legislative power to cover the field, including in the state and territory public sectors; and

- the new *Privacy (Credit Reporting Information) Regulations*, to assess whether the policy objectives underpinning the regulations are being achieved.

In addition, some matters were considered by the ALRC to be outside the scope of this Inquiry. When considered appropriate, the ALRC has recommended a further inquiry or study. Examples include the recommendations that the Australian Government:

- undertake an inquiry to consider whether appropriate legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take;[27]

- fund a longitudinal study of the attitudes of Australians, in particular young people, to privacy;[28] and

- initiate a review to consider whether the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies.[29]

27 See Ch 7.
28 See Ch 67.
29 See Ch 71.

Part A

Introduction

1. Introduction to the Inquiry

Contents

Introduction

1.1 On 30 January 2006, the then Attorney-General, the Hon Philip Ruddock MP, asked the Australian Law Reform Commission (ALRC) to conduct an inquiry into the

extent to which the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia.[1] During the course of the Inquiry, the ALRC published two Issues Papers, *Review of Privacy* (IP 31)[2] and *Review of Privacy—Credit Reporting Provisions* (IP 32),[3] and a three volume discussion paper, *Review of Australian Privacy Law* (DP 72). To facilitate community involvement, concise overviews of the Issues Papers[4] and the Discussion Paper[5] were published. An interactive website, 'Talking Privacy', was designed specially for children and young people, and was accessible from the ALRC's homepage.

1.2 The *Privacy Act* itself is substantially the product of a seven-year research effort by the ALRC, which culminated in 1983 with the three volume report, *Privacy* (ALRC 22).[6] The Act also gave effect to Australia's obligations to implement the Organisation for Economic Co-operation and Development *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines),[7] and partially implemented into domestic law Australia's obligations under art 17 of the *International Covenant on Civil and Political Rights* (ICCPR).[8]

Background

ALRC 22

1.3 In April 1976, the ALRC received a wide-ranging reference on privacy. Due to particular public concerns at the time, a separate Discussion Paper and Report were completed on access to census records.[9] Two discussion papers were produced—in 1977 and 1980[10]—and the final Report, *Privacy* (ALRC 22), was tabled in Parliament in December 1983. Volume 1 of that Report provides a discussion of the issues; the

---

1 Such a review was recommended in two previous inquiries: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 2; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 1.

2 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).

3 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006).

4 Australian Law Reform Commission, *Reviewing Australia's Privacy Laws: Is Privacy Passé?*, Overview (2006).

5 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007).

6 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

7 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed below, and in detail in Part D.

8 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [2.54]. Article 17 of the ICCPR provides: '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks': *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

9 Australian Law Reform Commission, *Privacy and the Census*, DP 8 (1978); Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).

10 Australian Law Reform Commission, *Privacy and Publication—Proposals for Protection*, DP 2 (1977); Australian Law Reform Commission, *Privacy and Intrusions*, DP 13 (1980).

ALRC's recommendations and draft legislation are found in Volume 2; and Volume 3 contains various appendices.[11]

1.4 ALRC 22 was not the first time the ALRC had to consider the concept of privacy. One earlier Report—*Unfair Publication: Defamation and Privacy* (ALRC 11)[12]—is worthy of particular note. In addition to making recommendations for reform in the law of defamation, ALRC 11 proposed some limited privacy protection. It was recommended that a person be allowed to sue for damages or an injunction

> if 'sensitive private facts', relating to health, private behaviour, home life, and personal or family relationships, were published about him which were likely in all the circumstances to cause distress, annoyance or embarrassment to a person in the position of the individual. Wide defences were proposed allowing publication of personal information if the publication was relevant to the topic of public interest.[13]

1.5 In ALRC 22, the ALRC identified dangers to privacy, including growing official powers, new business practices (such as electronic surveillance, credit reporting and direct marketing), and concerns associated with new information technology. Instead of advocating a single approach to privacy, the ALRC's recommendations targeted a number of different areas in which privacy concerns were identified.

1.6 In formulating its recommendations for legislative reform, the ALRC divided privacy questions into two broad categories—those relating to intrusions, and those relating to information handling. The ALRC subdivided the first category into two broad sub-categories: personal and property intrusions; and intrusions caused by spying and the interception of communications. The ALRC noted, however, that these sub-categories were 'not necessarily mutually exclusive'.[14]

1.7 Many of the recommendations relating to information privacy contained in ALRC 22 subsequently found their way into the *Privacy Act*. In particular:

- a 'permanent statutory guardian for privacy',[15] the Privacy Commissioner, was created;

---

11 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Appendix B, Bibliography on the Concept of Privacy; Appendix C, Tables of Commonwealth and ACT Legislation Conferring Powers of Arrest and Detention, Entry and Search, and Access to, and Production of, Information; Appendix D, Overseas Information Privacy Laws; Appendix E, Laws Regulating Interception of Oral and Written Communication; Appendix F, Course of the Inquiry.

12 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979).

13 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [6]. See generally Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [250]. How far Australia has progressed in recognising a common law right to privacy since the publication of ALRC 11 is discussed in Part K.

14 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1093].

15 Ibid, xliii.

- statutory privacy principles 'to aid the Privacy Commissioner in the evaluation of complaints about privacy invasion … in respect of … misuse of personal information'[16] were given legislative force;

- access to, and an ability to correct, credit information was provided for; and

- rules governing the use, disclosure and security of some forms of personal information were implemented.

1.8 In IP 31, the recommendations in ALRC 22 relating to intrusions, and significant developments in the regulation of intrusions in the intervening period, were outlined.[17] While the scope of the current Inquiry is not as broad as ALRC 22,[18] the extraordinary advances in information technology have greatly expanded the contexts and concerns about information privacy that are dealt with in this Report.

1.9 As a general matter, intrusions only will be discussed in this Report if they involve information collection, use and disclosure of personal information. Legislative initiatives authorising intrusions, or designed to control unsolicited communications,[19] will be considered if they are inconsistent with the provisions of the *Privacy Act*, and the ALRC's recommendations for reform of that Act. Further, to the extent that the intrusion constitutes a serious invasion of privacy, the proposed statutory cause of action may apply. The cause of action is discussed in detail in Part K.

OECD Guidelines

1.10 On 23 September 1980, the Council of the OECD adopted guidelines governing the protection of privacy and transborder flows of information.[20] The OECD Guidelines were developed to facilitate the harmonisation of national privacy legislation of OECD member countries, and, while upholding human rights, to prevent interruption in the international flow of personal information.[21]

1.11 The OECD Expert Group on Privacy Principles (1978–1980) was headed by then ALRC Chair Justice Michael Kirby, so that the ALRC's work in this field strongly influenced the development of the law internationally. Justice Kirby also chaired the OECD's Expert Group on Data Security (1991–1992).

---

16 Ibid, xliii.

17 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [1.12]–[1.40].

18 See discussion of the scope of this Inquiry below.

19 The *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth) are examples of legislation designed to control unsolicited communications.

20 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

21 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [602]. Levin and Nicholson note that the OECD Guidelines were the product of the Council of Europe's efforts, immediately after its inception in 1949, to address the issue of personal information in 'the aftermath of World War II and its horrors': A Levin and M Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005) 2 *University of Ottawa Law and Technology Journal* 357, 374.

1.12 Eight basic principles of national application are set out in Part Two of the OECD Guidelines:[22]

> **Collection Limitation Principle**—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> **Data Quality Principle**—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> **Purpose Specification Principle**—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> **Use Limitation Principle**—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
>
> a) with the consent of the data subject; or
>
> b) by the authority of law.
>
> **Security Safeguards Principle**—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
>
> **Openness Principle**—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> **Individual Participation Principle**—An individual should have the right:
>
> a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
>
> b) to have communicated to him, data relating to him
>
> - 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;
>
> c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
>
> d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> **Accountability Principle**—A data controller should be accountable for complying with measures which give effect to the principles stated above.

---

22 The full text of the OECD Guidelines can be found at <www.oecd.org>.

1.13 The OECD Guidelines, and subsequent models to facilitate cross-border data protection, are discussed in detail in Part D.

Privacy Act

1.14 The *Privacy Act* regulates the handling of personal information. Initially, the Act applied exclusively to the Commonwealth public sector. Public sector agencies are required to comply with the Information Privacy Principles (IPPs), which are similar, but not identical, to the OECD Guidelines. The Act was amended shortly after its enactment 'to deal with government data-matching activities and the activities of credit providers and also was extended to cover the Australian Capital Territory public sector'. [23]

1.15 In 2000, amendments to the *Privacy Act* established a separate set of privacy principles, known as the National Privacy Principles (NPPs), which apply to the private sector.[24] The IPPs and the NPPs are discussed in detail in Part D. A general overview of the *Privacy Act* is provided in Chapter 5.

The scope of the Inquiry

Terms of Reference

1.16 The Terms of Reference, reproduced at the beginning of this Report, direct the ALRC to focus on the extent to which the *Privacy Act* and related laws continue to provide an effective framework for the protection of privacy in Australia. Four factors relevant to the decision to initiate the Inquiry were identified:

- rapid advances in information, communication, storage, surveillance and other relevant technologies;
- possible changing community perceptions of privacy and the extent to which privacy should be protected by legislation;
- the expansion of state and territory legislative activity in areas relevant to privacy; and
- emerging areas that may require privacy protection.

1.17 During the course of the Inquiry, the ALRC was asked to consider:

- relevant existing and proposed Commonwealth, state and territory laws and practices;

---

23 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [2.54]. The credit reporting provisions are discussed in detail in Part G.

24 *Privacy Amendment (Private Sector) Act 2000* (Cth), which came into effect on 21 December 2001.

- other recent reviews of the *Privacy Act*;
- current and emerging international law and obligations in the privacy area;
- privacy regimes, developments and trends in other jurisdictions;
- any relevant constitutional issue;
- the need of individuals for privacy protection in an evolving technological environment;
- the desirability of minimising the regulatory burden on business in the privacy area; and
- any other related matter.

1.18 The ALRC was asked to identify and consult with relevant stakeholders, including the Office of the Privacy Commissioner (OPC), relevant state and territory bodies and the Australian business community, as well as to ensure widespread public engagement with the Inquiry.

1.19 The Terms of Reference initially specified that the ALRC deliver the final Report to the Attorney-General by 31 March 2008. On 24 January 2008, the ALRC formally requested an extension, occasioned partly by the size and complexity of the Inquiry, but mainly by the difficulty stakeholders were experiencing in providing submissions on DP 72 in a timely fashion.[25] In a letter dated 11 February 2008, the Attorney-General, the Hon Robert McClelland MP, agreed to extend the reporting date for the Inquiry to 30 May 2008.

Related privacy inquiries

1.20 During the course of this Inquiry, the Victorian Law Reform Commission (VLRC), the New South Wales Law Reform Commission (NSWLRC) and the New Zealand Law Commission (NZLC) also conducted privacy inquiries. These Commissions and the ALRC produced separate consultation papers and final reports, but worked closely and cooperatively, sharing ideas, information and a number of consultation meetings.

25 Approximately 200 submissions were received by the ALRC after the 7 December 2007 closing date for submissions on DP 72. In particular, the federal election held in November 2007 made it difficult for some federal agencies to provide their submissions by the closing date.

VLRC privacy inquiries

1.21 In March 2002, the VLRC was asked to examine two issues of public concern relating to privacy: workplace privacy and privacy in public places.[26]

Workplace privacy

1.22 The VLRC completed its inquiry into workplace privacy in 2005. The *Workplace Privacy: Final Report* considered the surveillance, monitoring, physical and psychological testing, and searching of workers, as well as the collection, use and disclosure of personal information in workers' records. [27] The report also included a draft Workplace Privacy Bill.[28]

1.23 The ALRC is advised that, at the time of writing this Report, the Standing Committee of Attorneys-General (SCAG) is considering the VLRC's report into workplace privacy and seeking to develop a consistent, national approach. Options for reform are being considered to regulate workplace surveillance (including email and internet monitoring), covert surveillance practices, surveillance and monitoring of employees outside of work, and genetic testing in the workplace, including the taking of bodily samples.

1.24 Apart from considering whether employee records should be exempt from the provisions of the *Privacy Act*,[29] the ALRC has not dealt specifically with workplace privacy in this Report, in order to avoid unnecessarily duplicating the work being undertaken by SCAG.

Surveillance in Public Places

1.25 A consultation paper focusing on surveillance in public places is scheduled for release by the VLRC in mid-2008. It is anticipated that the final report will be completed by the end of 2008.

1.26 While the privacy implications of surveillance are considered in a variety of places in this Report—for example, the telecommunications context is considered in Part J, and the protection of a right to personal privacy is considered in Part K—the ALRC has not focused specifically on the issue.

---

26 Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004), [1.1]. The Terms of Reference can be found at <www.lawreform.vic.gov.au>.

27 See Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005); Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004); Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002).

28 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), Appendix 5.

29 The use and disclosure of workers' personal information is discussed in Ch 40.

NSWLRC privacy inquiry

1.27 On 11 April 2006, the Attorney General of New South Wales asked the NSWLRC to inquire into and report on whether existing state legislation provides an effective framework for the protection of the privacy of an individual. In undertaking the review, the NSWLRC was directed to consider:

- the desirability of privacy protection principles being uniform across Australia;
- the desirability of a consistent legislative approach to privacy in the *Privacy and Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Protection Act 2002* (NSW), *State Records Act 1998* (NSW), *Freedom of Information Act 1989* (NSW) and *Local Government Act 1993* (NSW);
- the desirability of introducing a statutory tort of privacy in New South Wales; and
- any related matters.

1.28 The NSWLRC also was directed to liaise with the ALRC and other relevant Commonwealth, state and territory agencies.

1.29 In May 2007, the NSWLRC released the first of the consultation papers to be published during the course of its inquiry. Consultation Paper 1, *Invasion of Privacy* (NSWLRC CP 1), addresses the desirability of introducing a statutory cause of action for invasion of privacy in New South Wales, and puts forward for consultation proposals for the introduction of such a cause of action. The NSWLRC intends to release a second consultation paper on the remaining aspects of its inquiry in mid-2008. A final report should be completed by the end of 2008**.** NSWLRC CP 1 is considered in detail in Part K of this Report.

NZLC privacy inquiry

1.30 The NZLC privacy review is proceeding in four stages. Stage one, which has been completed, was a high level policy overview which considered privacy values, changes in technology, international trends, and their implications for New Zealand law.[30] In stage two, which also has been completed,[31] the NZLC considered 'whether the law relating to public registers requires systematic alteration as a result of privacy considerations and emerging technology'. In stage three, 'the Commission will

30 Two documents were produced in this stage of the inquiry: M Hickford, *A Conceptual Approach to Privacy: Miscellaneous Paper 19* (2007) New Zealand Law Commission; New Zealand Law Commission, *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1*, Study Paper 19 (2008).

31 New Zealand Law Commission, *Public Registers—Review of the Law of Privacy, Stage 2*, Report 101 (2008).

consider and report on the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy'. A review and update of the *Privacy Act 1993* (NZ) will constitute stage four.[32] The Terms of Reference for the NZLC privacy review do not specify a reporting date for the projects.

The meaning of privacy

1.31 It has been suggested that privacy can be divided into a number of separate, but related, concepts:

> **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection';
>
> **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
>
> **Privacy of communications**, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
>
> **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.[33]

1.32 As the preceding discussion illustrates, the issues to be covered in this Inquiry do not fall neatly into one concept. The primary focus of this Report, however, is on information privacy.

1.33 The recognition of a general right to privacy warranting legal protection is a relatively modern phenomenon.[34] The genesis of modern legal academic discussion of the topic is generally acknowledged to be Samuel Warren and Louis Brandeis's article, 'The Right to Privacy' published in the *Harvard Law Review* in 1890.[35] Widespread debate, fuelled by the storage of personal information in computer data banks, commenced in the 1960s.[36]

---

32 New Zealand Law Commission, *Review of Privacy* (2006) <www.lawcom.govt.nz/ProjectGeneral.aspx?ProjectID=129> at 5 May 2008. All four stages are described in detail in the Terms of Reference, which can be found on the NZLRC's website.

33 D Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments* Privacy International <www.privacyinternational.org/survey/phr2000/overview.html> at 5 May 2008.

34 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 465.

35 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

36 See, eg, R Prosser, 'Privacy' (1960) 48 *California Law Review* 383; E Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962; C Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475. This is not to suggest an absence of legal discourse between the late 19th century and the 1960s. For example, see the articles cited in E Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962, n 4. See also J Stephen, *Liberty, Equality, Fraternity* (1967 ed, 1873), 160.

1.34 Writing in 1980, Professor Ruth Gavison argued that the modern concern for the protection of privacy can be attributed primarily to

> a change in the nature and magnitude of threats to privacy, due at least in part to technological change … Advances in the technology of surveillance and the recording, storage, and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed.[37]

1.35 Other factors, according to Gavison, include the advent of tabloid journalism, and the 'tendency to put old claims in new terms'.[38]

1.36 A new surge of academic comment on privacy, caused mainly by the growth of the internet, occurred in the 1990s.[39] Today, unprecedented advances in technology continue to fuel privacy-related fears—and are discussed in detail in Part B.

1.37 In ALRC 22, the ALRC indicated that the chief threats to privacy in Australia included:

> *Growing Official Powers*. The powers of increasing numbers of public officials to intrude into the lives and property of Australians are growing.
>
> *New Business Practices*. New intrusive practices have developed in recent years, such as electronic surveillance, credit reporting and direct marketing.
>
> *New Information Technology*. The computerisation of personal information has enormous advantages, but it also presents Australian society with new dangers, now well documented and understood.[40]

1.38 As evidenced by the Terms of Reference for this Inquiry, the ALRC's analysis was prescient and all of these factors resonate with equal, if not greater, force today.

Scope of privacy

1.39 Why is privacy considered important? What is the nature of the legal 'right' requiring protection? Professor Roger Clarke suggests that the importance of privacy has psychological, sociological, economic and political dimensions.

> **Psychologically**, people need private space. This applies in public as well as behind closed doors and drawn curtains …
>
> **Sociologically**, people need to be free to behave, and to associate with others, subject to broad social mores, but without the continual threat of being observed …

---

37 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 465. See also, D Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131, 135–136; M Jackson, *Hughes on Data Protection in Australia* (2nd ed, 2001), 10.

38 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 466.

39 See, eg, A Samuels, 'Privacy: Statutorily Definable?' (1996) 17 *Statute Law Review* 115; L Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' (1997) 28 *Metaphilosophy* 259; D Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087.

40 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), xli.

> **Economically**, people need to be free to innovate …
>
> **[P]olitically**, people need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and threatens democracy.[41]

1.40 In the Canadian Supreme Court case of *Vickery v Nova Scotia Supreme Court (Prothonotary)*, Cory J expressed a similar view, describing privacy as a right which

> inheres in the basic dignity of the individual. This right is of intrinsic importance to the fulfilment of each person, both individually and as a member of society. Without privacy it is difficult for an individual to possess and retain a sense of self-worth or to maintain an independence of spirit and thought.[42]

1.41 Ascertaining the scope of the legal 'right' is a more difficult task. Despite the best efforts of legal scholars, the term 'privacy' confounds attempts at delivering a universal definition.[43] In ALRC 22, it was noted that 'the very term "privacy" is one fraught with difficulty. The concept is an elusive one'.[44] Professor J Thomas McCarthy has noted:

> It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts … Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.[45]

1.42 In ALRC 22, the ALRC adopted a definition of the term 'privacy' that 'stayed as close as possible … to the ordinary language concept'.[46] This approach was criticised by Senator Brett Mason, who argues in this regard that ALRC 22 'is stronger on the practical application of legal rules and remedies to certain privacy issues than it is on theoretical analysis'.[47] He concludes that 'the ordinary language concept of "privacy" … does not necessarily inform a sensible legal right'.[48]

---

41 R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 5 May 2008. See also, E Barendt, 'Privacy and Freedom of Speech' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 11, 30–31.

42 *Vickery v Nova Scotia Supreme Court (Prothonotary)* [1991] 1 SCR 671, 687.

43 L Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' (1997) 28 *Metaphilosophy* 259. One commentator suggests that a reason the legal definition of privacy is so elusive is due to the fact that 'privacy has generally much more to do with politics than with law': B Mason, *Privacy Without Principle* (2006), xii.

44 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [19].

45 J McCarthy, *The Rights of Publicity and Privacy* (2nd ed, 2005), [5.59]. See also, D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 479.

46 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [20].

47 B Mason, *Privacy Without Principle* (2006), 40.

48 Ibid, 41.

1.43 Comparing American, French and German approaches to privacy, Professor James Whitman suggests that 'there is no such thing as privacy as such',[49] and maintains that:

> Americans and Europeans certainly do sometimes arrive at the same conclusions. Nevertheless, they have different starting points and different ultimate understandings of what counts as a just society … American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity. There are certainly times when the two bodies of law approach each other more or less nearly. Yet they are constantly pulled in different directions, and the consequence is that these two legal orders really do meaningfully differ: continental Europeans are consistently more drawn to problems touching on human dignity, while Americans are consistently more drawn to problems touching on the depredations of the state.[50]

1.44 Whitman argues that at the core of the European approach to privacy law is 'the right to control your public image—rights to guarantee that people see you the way you want to be seen'.[51] By contrast, the conceptual core of the American right to privacy is, according to Whitman, the 'right to freedom from intrusions by the state, especially in one's own home'.[52]

1.45 Whitman emphasises that the differences between American and European privacy law are comparative, not absolute.[53] It is possible to argue that 'protecting privacy means both safeguarding the presentation of self and inhibiting the investigative and regulatory excesses of the state'.[54] In practice, however, the differences are real.

1.46 Privacy expert Martin Abrams similarly observes that:

> Privacy law is culturally based. Privacy is considered a fundamental human right in Europe, highly regarded with pragmatic interest in the United States, and is only beginning to emerge as a topic in Asia. What works in one country or region doesn't always work in the other.[55]

1.47 This Inquiry has been directed by its Terms of Reference to focus specifically on 'matters relating to the extent to which the *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia'. Despite

---

49 J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 1151, 1221.

50 Ibid, 1163. See also, R Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 569.

51 J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 1151, 1161.

52 Ibid, 1161. The origins of the 'conceptual core', according to Professor Whitman, are the Fourth Amendment—the right against unlawful search and seizures: Ibid, 1212.

53 Ibid, 1203.

54 Ibid, 1219.

55 M Abrams, 'Privacy, Security and Economic Growth in an Emerging Digital Economy' (Paper presented at Privacy Symposium, Institute of Law China Academy of Social Science, 7 June 2006), 18.

the general title, as noted above, the *Privacy Act* is concerned almost exclusively with information privacy. In this context, Professor Margaret Jackson notes that 'one may query whether it is possible to advance a discussion of the adequacy of the law as a regulator of information privacy if one does not define the privacy interests at risk'.[56]

1.48 Consequently, there is some utility in attempting to identify, if not a 'core' or precise definition of universal application, at least an understanding of the way the term 'privacy' is being used in the context of this Inquiry. To achieve this objective, the ALRC convened a workshop with many of the leading Australian experts in the field. This discussion was useful in articulating the approach the ALRC should adopt when tackling the elusive concept of privacy.[57]

Towards a working definition

1.49 Professor Gavison suggests that 'privacy' is 'a term used with many meanings',[58] giving rise to two important questions.

> The first relates to the *status* of the term: is privacy a situation, a right, a claim, a form of control, a value? The second relates to the *characteristics* of privacy: is it related to information, to autonomy, to personal identity, to physical access? Support for all of these possible answers can be found in the literature.[59]

1.50 As a first step in coming to terms with the concept of 'privacy', it is important to recognise that the international community accords privacy the status of a human right through such key documents as the *Universal Declaration of Human Rights*,[60] and the ICCPR.[61] Australia signed the ICCPR on 18 December 1972 and ratified it on 13 August 1980. While 'the rights and obligations contained in the ICCPR are not incorporated into Australian law unless and until specific legislation is passed implementing the provisions',[62] the ICCPR's recognition of privacy as a human right lends support to the argument that such recognition is warranted in domestic law.

---

56 M Jackson, *Hughes on Data Protection in Australia* (2nd ed, 2001), 6.

57 The workshop participants included Professor Des Butler; Professor Roger Clarke; Professor David Kinley; Mr David Lindsay; Associate Professor Megan Richardson; and Dr Greg Taylor.

58 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 424.

59 Ibid, 424.

60 Article 12 provides: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks': *United Nations Universal Declaration of Human Rights*, GA Res 217A(III), UN Doc A/Res/810 (1948).

61 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

62 *Dietrich v The Queen* (1992) 177 CLR 292, 305.

1.51 Recently enacted domestic human rights legislation also recognises privacy as a basic human right. For example, s 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) provides:

> **Privacy and reputation**
>
> A person has the right—
>
> (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with;

1.52 The *Human Rights Act 2004* (ACT) contains an almost identical provision.[63] While such instruments include privacy in the list of rights accorded the status of a 'human right', they do not define the term, nor do they delineate the extent to which its scope intertwines with other freedoms, rights and interests.[64]

Status of privacy

1.53 The VLRC's *Workplace Privacy: Issues Paper* proposed that 'privacy can be expressed as a right, and that this *right* to privacy can then form the basis for determining what are legitimate *interests* in privacy'.[65] The VLRC formulated a working definition of privacy in terms of what the right to privacy encompasses, namely the right:

- 'not to be turned into an object or thing'; and
- 'not to be deprived of the capacity to form and develop relationships'.[66]

1.54 The NZLC adopted a blended 'core values' and 'harms to privacy' approach. The 'core values' approach recognises 'privacy as a sub-category of two interconnected core values'—namely, the autonomy of humans to live a life of their choosing; and the equal entitlement of humans to respect.[67] The 'harms to privacy' approach draws primarily on the work of Professor Daniel Solove, which is discussed in greater detail below.

1.55 In *R v Broadcasting Standards Commission ex parte BBC*, Lord Mustill attempted to define the essence of privacy as follows:

> To my mind the privacy of a human being denotes at the same time the personal 'space' in which the individual is free to be itself, and also the carapace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from

---

63 *Human Rights Act 2004* (ACT) s 12.

64 R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 5 May 2008.

65 Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002), xii (emphasis in original).

66 Ibid, [2.38]. Based on this working definition, the VLRC suggested that 'a test of invasion of privacy would be an assessment of the extent to which any particular law or practice has the effect of depriving people generally of [the right not to be reduced to an object and the right to relationships]': Ibid, [2.49].

67 New Zealand Law Commission, *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1*, Study Paper 19 (2008), [3.10].

> intrusion. An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate.[68]

1.56 Put another way, privacy may be viewed as the bundle of interests that individuals have in their personal sphere free from interference from others.[69] In this formulation, the use of the term 'interest' rather than 'right' is intentional and important. While privacy is a 'right' in a legal sense, for definitional purposes, the word 'interest' may be more accurate. A right is always an interest, even if not all interests are accorded the status of legal rights.

1.57 It is important to bear in mind that privacy interests unavoidably will compete, collide and coexist with other interests. For example, privacy often competes with freedom of expression, a child's right to protection from abuse, national security and so on. No single interest—not even one elevated to the status of a human right—is absolute.[70]

1.58 The Community Services Ministers' Advisory Council's submission to the Inquiry highlights the practical importance of the recognition of competing interests.

> Privacy is an important individual right. However, this does not stand alone: people also have other rights (to shelter, safety and care) and sometimes the exercise of rights on behalf of one person can have negative consequences for another person. Community services departments and agencies, with duty of care and statutory obligations to protect the vulnerable, are constantly seeking to mediate between competing rights and obligations.[71]

1.59 In a different context, Eady J considered the tension between freedom of expression and the privacy rights of an individual in *McKennitt v Ash*:

> It is clear that [in the United Kingdom] there is a significant shift taking place as between, on the one hand, freedom of expression for the media and the corresponding interest of the public to receive information, and, on the other hand, the legitimate expectation of citizens to have their private lives protected … Even where there is a genuine public interest, alongside a commercial interest in the media in publishing articles or photographs, sometimes such interests would have to yield to the individual citizen's right to the effective protection of private life.[72]

1.60 Ascertaining the appropriate policy to deal with the tension between competing interests is the challenge facing judges, legislators and law reformers. It follows from the above discussion that the status accorded to privacy—and in particular the status accorded to privacy in international and domestic human rights instruments—means

---

68 *R v Broadcasting Standards Commission ex parte BBC* [2001] QB 885, [48].

69 See eg R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 5 May 2008.

70 C Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475, 478. See also *Privacy Act 1988* (Cth) s 29(a).

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

72 *McKennitt v Ash* [2005] EMLR 10, [57]. The balancing of privacy and freedom of expression is discussed in greater detail in Part K.

that privacy interests will usually take precedence over less fundamental interests, such as economic choice and opportunity.[73]

1.61 For example, an argument for greater access to personal information based on reduced cost to custodians of personal information, or customer convenience, generally will not tilt the balance in favour of reduced privacy protection—at least in the absence of other compelling factors. Conversely, an argument that the use of personal information will lead to an increase in an individual's standard of living may warrant a reduced level of privacy protection, given that standard of living is directly related to the health and wellbeing of an individual or the individual's family—a recognised human right.[74]

Characteristics of privacy

1.62 Identifying the characteristics of privacy is conceptually more difficult than ascertaining its status. Professor Solove suggests that attempts to identify the essential characteristics of privacy—that is, the common denominators that make things private—are misguided. Solove argues that:

> the top-down approach of beginning with an over-arching conception of privacy designed to apply in all contexts often results in a conception that does not fit well when applied to a multitude of situations and problems involving privacy.[75]

1.63 Instead, Solove advocates a more pragmatic, bottom-up, approach.

> We should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them. If privacy is conceptualized as a web of interconnected types of disruption of specific practices, then the act of conceptualizing privacy should consist of mapping the topography of the web. We can focus on particular points of the web. These 'focal points' are not categories, and they do not have fixed boundaries.[76]

1.64 Some critics, however, reject the pragmatic approach. For example, Professor Richard Bruyer argues that:

> Unless a common denominator is articulated, combining conceptions simply perpetuates the piecemeal, haphazard approach to privacy that has marked the privacy landscape so far. Nor will it provide a satisfactory answer for the hard privacy cases as they occur.[77]

---

73 M Abrams, 'Privacy, Security and Economic Growth in an Emerging Digital Economy' (Paper presented at Privacy Symposium, Institute of Law China Academy of Social Science, 7 June 2006), 9.

74 *United Nations Universal Declaration of Human Rights*, GA Res 217A(III), UN Doc A/Res/810 (1948), art 25.

75 D Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1099.

76 Ibid, 1130.

77 R Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 576.

1.65 The NZLC suggests that 'the main shortcoming of Solove's approach is that it provides no basis for establishing why some harms are privacy violations and others are not'.[78]

1.66 The characteristics of privacy also may have a changing demographic dimension. For example, what 'Builders' and 'Baby Boomers' see as necessarily falling within the 'topography of the web' may not resonate with 'Generations X, Y and Z'.[79] Young people appear much more willing to share personal details, post images and interact with others on internet chat sites.[80] Whether this indicates a fundamental shift in attitudes to privacy—or simply the cavalier attitude and excesses of youth displayed in a new form—is an open question.[81]

1.67 The pragmatic approach advocated by theorists such as Solove provides a useful template for law reform. Rather than focusing on an overarching definition of privacy, it makes more sense, using Solove's terminology, to focus on particular points in the web and formulate a workable approach to deal with the disruption.[82]

1.68 In this Inquiry, the ALRC has been asked to review an existing piece of legislation, the *Privacy Act*—which deals with information privacy—and to consider emerging areas that may require privacy protection. The 'focal points' of inquiry largely have been delineated by the legislation, and the reform needed to address any disruptions to specific practices can be articulated with reference to the legislation. In the case of emerging areas that require privacy protection—and in particular those areas falling within the scope of the statutory cause of action for a serious invasion of privacy discussed in detail in Part K——the disruption to specific practices can be identified with reference to case law, academic comment and legislation. In addition, the 'blended core values approach' articulated by the NZLC, discussed above, helps to determine whether a specific disruption falls within the penumbra of privacy.

Information privacy: the commercial context

1.69 Most people think about information privacy in terms of the collection and use of their personal information—most likely based on a one-to-one relationship with the agency or organisation concerned. Modern information technology, however, greatly facilitates the collection, aggregation, systematisation and matching of vast amounts of data, acquired from large numbers of individuals, with or without their consent—or even their awareness.

---

78 New Zealand Law Commission, *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1*, Study Paper 19 (2008), [2.37].

79 For a discussion of the age limits of the generational categories, see Part I.

80 L Weeks, 'See Me, Click Me: The Publizen's Life? It's an Open Blog. The Idea He May be Overexposed? LOL', *Washington Post* (online), 23 July 2006, <www.washingtonpost.com>.

81 This is discussed in more detail in Ch 69.

82 D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 485–486.

1.70 Database construction may occur for a variety of reasons. For example, human genetic research has now moved beyond the 'mapping' or 'sequencing' of an individual genome (the goal of the historic Human Genome Project) to scanning DNA profiles from many thousands of people, in order to identify genetic variations that might be associated with common but complex health problems (such as diabetes, degenerative nerve diseases and cancers). A number of countries and regions have established (or proposed) large databases of genetic information and tissue samples—often referred to as 'biobanks'—to pursue this sort of 'population genomics'. The UK Biobank already has collected over 100,000 samples from volunteer participants, with a target of 500,000.[83] Obviously, such collections of sensitive personal information require the highest standards of ethical oversight and governance, including regard for individual privacy.[84]

1.71 The accumulation and 'mining' of large databases containing other forms of personal information—such as property holdings, financial transactions, credit worthiness[85] and consumer preferences—also has tremendous value for various commercial and direct marketing[86] purposes. This is particularly relevant in an era characterised by globalisation and the massive growth of the internet and e-commerce. Veda Advantage submitted that:

> Information networks are now the rapidly growing core of the information economy. Large fixed and variable data networks now operate across the finance, travel, health and telecommunications industries. Our credit reporting system was one of the earliest and largest information networks in Australia and gives real experience of the challenges of data protection and business efficiency in this information age.[87]

1.72 Veda also noted that 'there are two worlds of data—direct and indirect', so that while a service provider organisation collects data directly from an individual, 'that organisation lives in two data worlds … transferring data to other organisations'. As a matter of course,

> these organisations have multiple relationships with each other, but do not have direct relationships with the individual data subject. In reality these relationships are [very complex]. They are also an essential part of the information economy …

---

83 As at 24 April 2008, the UK Biobank website reported 106,482 recruits; see: <www.ukbiobank.ac.uk>.

84 See Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), especially Part E: Human Genetic Databases (chs 18–20); see also D Chalmers, 'International Co-operation Between Biobanks: The Case for Harmonisation of Guidelines and Governance' in M Stranger (ed) *Human Biotechnology & Public Trust: Trends, Perceptions and Regulation* (2007) 237, 240-241. The United Kingdom's National DNA Database (NDNAD)—managed by the police and used for criminal investigations and other forensic purposes (such as identification)—holds DNA profiles relating to over 4.3 million individuals, increasing at a rate of about 2,000 per week and amounting to about six per cent of the total population: see GeneWatch UK, *The UK Police National DNA Database* <www.genewatch.org/sub-539478> at 24 April 2008

85 See Part G.

86 See Ch 26.

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

> Our submission is drawn from experience with the large, networked data sets collected, analysed and shared among corporations. The technologies, business processes and regulation that cover organisations which collect, collate, mine and network information are now relatively mature.[88]

1.73 Indeed, and not surprisingly, the information economy has given rise to major corporations that provide services almost entirely based on the collection and strategic mining and analysis of data. For example, the giant Acxiom Corporation, based in the United States, promotes itself as

> a global leader in helping companies maximize the value of information. Our innovative information management solutions provide critical insights into consumers that help companies acquire and build stronger, more profitable relationships with their customers … When companies work with Acxiom, we make it easy for them to establish strong ties with customers by helping them better understand what customers like, what they want and the best ways to communicate with them. Acxiom's customer information management solutions help close gaps in customer knowledge—a key to our clients' ability to sustain and grow their businesses.[89]

1.74 Among other things, Acxiom offers services relating to information management, direct marketing strategies, online marketing, and improving the privacy and security of customer information.[90] As the oft-repeated slogan goes, 'privacy is good business'—that is, consumer trust is a *sine qua non* of engagement with such services as e-commerce and internet banking.

1.75 In Australia, Ticketek established a joint venture with Veda Advantage, aimed at generating revenue by providing marketers with access to a 'permission-based' database of consumers joining the Ticketek Rewards program. According to the executive in charge of the program, it is projected to grow to 150,000 or 200,000 individuals by the end of 2008,

> making it one of Australia's largest online research panels. It is growing rapidly ... It's becoming a big panel and, just as importantly, a quality panel. It skews to people with high disposable income and, unlike some other online consumer panels, we know that Ticketek Rewards members are real customers who spend money.[91]

1.76 Another good example of the shifting nature of service provision in the 'information age' is the recent trend of companies selling off, or selling significant stakes in, their loyalty programs. Air Canada was the first to do this, floating 35 per cent of its Aeroplan frequent flyer program in 2003[92]—which, remarkably, is now more highly capitalised than the airline itself.[93] Qantas also is looking at floating a

---

88 Ibid.

89 See Acxiom Corporation, *Overview* <www.acxiom.com/overview> at 23 April 2008.

90 Ibid.

91 N Shoebridge, 'Ticketek Lets Veda Pop the Question', *Australian Financial Review*, 21 April 2008, 51.

92 B Simon, 'Air Canada Selling Stake in Customer Reward Plan', *New York Times* (online), 28 January 2003, <www.nytimes.com>.

93 E Knight, 'Frequent Flyers for Sale—The Ultimate Reward for Qantas', *Sydney Morning Herald* (online), 21 March 2008, <www.smh.com.au>.

significant minority share in its Qantas frequent flyers program, with brokers estimating in March 2008 that Qantas frequent flyers is worth up to $2 billion, or about a quarter of the market capitalisation of the airline itself.[94]

1.77 The high stand-alone value of these loyalty programs is attributable almost entirely to the size and nature of the databases holding the personal information of their customers. Frequent flyer programs are particularly prized because their lists contain many people who are high net worth individuals, or at least substantial spenders.

> One of the reasons the Aeroplan business [was] considered more valuable than the airline that once owned it is that the market applies a much larger multiple to the loyalty company's earnings. This is because investors see growth opportunities in these reward programs and they see more reliable and less volatile earnings.[95]

1.78 In the course of the Inquiry, the ALRC found that a good deal of the debate about privacy protection in the business community was focused on the compliance burden. To the extent that this reflects the unnecessary complexity of the current legal regime, it is understandable—and in this Report, a central thrust of the ALRC's recommendations is to simplify greatly and harmonise the law in this area, with the aim of reducing the compliance burden.

1.79 However, compliance with basic information privacy principles should not be seen as a punishment—it accords with commercial best practice standards and, in most cases, with basic common sense. Most critically, consumers do, and should be entitled to, expect that their personal information will be treated with due care and respect. As the mantra goes, 'privacy is good for business', and information can be the basis of 'big business'. The commercial context of privacy must be considered carefully in the law reform process.

Process of reform

Advisory Committee and Sub-committees

1.80 It is standard operating procedure for the ALRC to establish an expert Advisory Committee to assist with the development of its inquiries.[96] In this Inquiry, the Advisory Committee includes current and former Privacy Commissioners; representatives from the business and government sector; privacy and consumer advocates; privacy professionals; health and social service professionals; academics and practising lawyers with expertise in privacy, health law and e-commerce; and public and private sector officers with responsibility for privacy-related issues. Given the breadth of this Inquiry, the ALRC also has established three Sub-committees of the

94 Ibid.
95 Ibid.
96 A list of Advisory Committee members can be found in the List of Participants at the front of this publication.

Advisory Committee in the areas of health privacy, developing technology and credit reporting.[97]

1.81 The Advisory Committee and Sub-committee members have particular value in helping the ALRC identify the key issues and stakeholders, as well as in providing quality assurance in the research and consultation effort. These committees also assisted with the development of questions and proposals for reform in the community consultation documents published by the ALRC during the course of the Inquiry. The Advisory Committee also assisted with formulation of the final recommendations contained in this Report. Ultimate responsibility for the final Report and recommendations, however, remains with the Commissioners of the ALRC.

Community consultation and participation

1.82 Under the terms of its constituting Act, the ALRC 'may inform itself in any way it thinks fit' for the purposes of reviewing or considering anything that is the subject of an inquiry.[98] One of the most important features of ALRC inquiries is the deep commitment to extensive community consultation.

1.83 There were several ways in which those with an interest in this Inquiry could participate. First, individuals and organisations could indicate an expression of interest in the Inquiry by contacting the ALRC or registering online at <www.alrc.gov.au>. Those who asked to be added to the ALRC's mailing list for this Inquiry received notices, press releases and a copy of each of the consultation documents published.

1.84 During the course of this Inquiry, the ALRC undertook its largest ever consultation program, conducting 250 meetings with individuals, public sector agencies, private organisations, community groups and peak associations. The consultations were designed to capture the views of a wide cross-section of interested stakeholders, including: corporations; privacy advocates; academics and lawyers with expertise in privacy; federal, state and territory government departments; state bodies such as the childrens' commissioners of New South Wales, Queensland and Tasmania; the Victorian Government Office of the Health Services Commissioner; federal, state and territory privacy commissioners; privacy commissioners from Canada, the United Kingdom, New Zealand, Hong Kong and Germany; business, consumer and health representatives; organisations and agencies representing children and young people; the Access Card Taskforce; the National Health and Medical Research Council; the Human Rights and Equal Opportunity Commission; and the Australian Institute of Aboriginal and Torres Strait Islander Studies. A list of those with whom the ALRC has consulted is found in Appendix 2 of this Report.

---

97 Lists of the members of the three sub-committees can be found in the List of Participants at the front of this publication.

98 *Australian Law Reform Commission Act 1996* (Cth) s 38.

1.85 In addition, the ALRC conducted a series of roundtables with individuals, agencies and organisations on a variety of themes including: credit reporting, exemptions under the *Privacy Act*; the privacy principles; children and young people; and health and research. The ALRC also organised well-advertised public forums in Melbourne (focusing on consumers and privacy), Sydney (focusing on business and privacy) and Coffs Harbour (focusing on health privacy and research). Finally, specially designed youth workshops (ages 13–25) were conducted in Sydney, Perth, Brisbane and Hobart.

1.86 Finally, individuals, organisations and federal, state and territory government agencies made written submissions. During the course of the Inquiry, 585 submissions were received by the ALRC—a complete list of submissions is found in Appendix 1 of the Report.

1.87 The ALRC is grateful for the outstanding contribution made to its work by stakeholders interested in the operation of the *Privacy Act* and other privacy-related legislation. Privacy regulation is an area in which strongly divergent views are expressed by individuals, public sector agencies, industry, consumer representatives and privacy advocates. Despite conflicting views about, and interests in, reform of privacy regulation, stakeholders engaged with the ALRC, and with each other, in a positive and constructive manner.

1.88 The stakeholders involved in the review of the credit reporting provisions, discussed in detail in Part G, warrant specific mention. Industry associations, especially the Australasian Retail Credit Association, were active in brokering a significant new consensus within the credit industry on a number of issues. In addition, consumer and industry representatives, and privacy advocates, engaged constructively in discussions related to reform of the credit reporting system. Through these discussions, positions were clarified and consensus on a number of important issues was reached.

ALRC National Privacy Phone-in

1.89 On 1 and 2 June 2006, members of the public were invited to contact the ALRC—either by telephone or via the ALRC's website—to share their experiences of privacy breaches and protection. The National Privacy Phone-in attracted widespread media coverage, and in total the ALRC received 1,343 responses.

1.90 The majority of respondents (73%) nominated telemarketing as their main concern.[99] Other prominent issues included:[100]

- handling of personal information by private companies (19%) and government agencies (9%);

---

99 This was possibly influenced by the fact that a number of media stories about the Phone-in focused on telemarketing as a possible concern.

100 Callers were able to nominate more than one concern, which is reflected in the statistics.

- protection of privacy in the internet age (7%);
- identity cards and smart cards (7%); and
- problems accessing and correcting personal information (7%).

1.91 The fact that callers could remain anonymous facilitated frank disclosure. The views expressed included support both for extending and reducing the scope of privacy protection, and provided useful examples of the impact of privacy law in a wide range of circumstances.

Talking Privacy Website

1.92 In early 2007, the ALRC developed a website called 'Talking Privacy', which was accessible from the ALRC's home page. Designed specifically to appeal to young people, the website contained information about the Inquiry, links to further information about privacy law, and encouraged young people to send in comments to the ALRC about their privacy issues or experiences. The site also contained information aimed at teachers and students considering law reform or privacy as part of a school curriculum.

1.93 The aim of the Talking Privacy website was to engage young people using a familiar and well-used medium. A number of young people took the step of submitting comments for consideration by the ALRC.

Organisation of this Report

1.94 This Report is divided into 11 parts and 74 chapters. The size of the Report reflects the breadth and complexity of this area of law. The structure adopted in this Report is designed to enable those with an interest in a particular area to refer directly to the part of the Report that deals with that area. Through reference to the Contents, part headings, chapter titles and index, relevant information can be found quickly.

1.95 The key findings and recommendations in this Report are summarised in the preceding Executive Summary. For ease of reference, a brief description of the material covered in each part follows below.

Part A–Introduction

1.96 Part A deals with introductory matters, the definition of the word 'privacy', an overview of privacy regulation in Australia and of the *Privacy Act*. Models for achieving national consistency, the regulatory model underpinning the recommendations in this Report, privacy beyond the individual—in particular Indigenous groups—and privacy of deceased individuals, are also discussed.

Part B–Developing Technology

1.97 Part B considers the impact on privacy of rapid advances in information, communication, storage, surveillance and other relevant technologies, and considers how best to accommodate developing technology in a regulatory framework. The impact of the internet, including how the internet has changed the nature of a 'public' space, and the prevalence of identity theft in an electronic environment, are also considered.

Part C–Interaction, Inconsistency and Fragmentation

1.98 Part C considers how the *Privacy Act* interacts with other federal, state and territory laws, and identifies areas of fragmentation and inconsistency in the regulation of personal information.

Part D–The Privacy Principles

1.99 Part D outlines the recommended reform of the privacy principles in the *Privacy Act*. Chapter 18 discusses the operation of the existing IPPs and NPPs, and focuses on how the structure of the privacy principles should be reformed. Chapter 19 considers the issue of consent as it applies to the privacy principles. Thereafter, the chapters are arranged thematically according to the 11 model Unified Privacy Principles (UPPs). In each chapter, there is a brief explanation of how the IPPs and NPPs currently apply, followed by recommendations for reform of the specific principle. A draft of the model UPPs, which is intended to illustrate for the statutory drafters the ALRC's approach to reform of the principles, is set out at the beginning of this Report.

Part E–Exemptions

1.100 In Part E, exemptions and partial exemptions to the *Privacy Act* are discussed.[101] Of particular note are the ALRC's recommendations to remove the exemptions for small business, employee records, political parties and political acts and practices.

Part F–Office of the Privacy Commissioner

1.101 Part F 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 Privacy Commissioner's functions of overseeing and monitoring compliance with the *Privacy Act* are considered; and the Commissioner's powers to issue Public Interest Determinations are discussed. Part F also includes recommendations for streamlining and increasing the effectiveness of complaint handling under the *Privacy Act*, and for the introduction of data breach notification provisions.

---

101 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: 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.

Part G–Credit Reporting Provisions

1.102 Part G examines the credit reporting provisions contained in Part IIIA of the *Privacy Act*. The legislative history of these provisions is outlined, followed by a discussion of the ALRC's recommendations for a system of more comprehensive credit reporting. This part also addresses specific aspects of the credit reporting system, such as collection, use and disclosure of credit reporting information, data quality and security, and rights of access, complaint handling and penalties.

Part H–Health Services and Research

1.103 Part H considers health information and research, including the need for greater national consistency in health privacy regulation as well as nationwide developments in relation to electronic health information systems. Relevant definitions—such as the definitions of 'health information' and 'health service'—and the additions and exceptions in the privacy principles that relate specifically to health information, are considered. The use of health information in the health services context, including the provision of health care and the management, funding and monitoring of health services, are also discussed. The special arrangements in place under the *Privacy Act* to allow for the use of personal information in health and medical research are examined, and a recommendation is made to extend these arrangements to include the use of personal information in areas of human research more generally.

Part I–Children, Young People and Adults Requiring Assistance

1.104 Part I focuses on children, young people and adults requiring assistance. The attitudes to privacy of children and young people are considered, and major challenges, such as online privacy and the taking and uploading of photographs, are discussed. The issue of decision making by individuals under the age of 18 is explored, and recommendations are made concerning age of the presumed capacity, consent, and handling of personal information of persons under the age of 18. A recommendation to introduce into the *Privacy Act* the concept of 'nominee' is made, and other issues concerning third party assistance with decision making are discussed.

Part J–Telecommunications

1.105 The focus of Part J is on telecommunications, and in particular the interaction between Part 13 of the *Telecommunications Act 1997* (Cth) and the *Privacy Act*. Whether telecommunications-specific privacy legislation is required, and whether Part 13 provides adequate protection of personal information, is explored. The role of the OPC and the Australian Communications and Media Authority under the *Telecommunications Act* also is considered. The interaction between the *Telecommunications Act* and other legislation—in particular the *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth)—is discussed.

Part K–Protection of a Right to Personal Privacy

1.106 Part K addresses the protection of a right to personal privacy. This part includes a discussion of developments towards recognising a right to personal privacy in Australia, and the ALRC's recommendation for a statutory cause of action for a serious invasion of privacy.

Further processes

1.107 Under s 23 of the *Australian Law Reform Commission Act 1996* (Cth), reports presented to the Attorney-General must be tabled in Parliament within 15 sitting days, after which they become public documents. This Report is not a self-executing document—the ALRC provides advice and recommendations about the best way to proceed, but implementation always is a matter for the Government and others to whom recommendations are directed.[102]

1.108 The ALRC's earlier report on privacy contained draft legislation, which formed the basis of the *Privacy Act*. Such draft legislation was typical of the law reform effort in those times. The ALRC's practice has changed, however, and draft bills are not produced unless specifically called for by the Terms of Reference. This is partly because drafting is a specialised function better left to the legislative drafting experts, and partly in recognition of the fact that the ALRC's time and resources are better directed towards developing the policy settings that will shape any resulting legislation.

1.109 The ALRC has not been asked to produce draft legislation in this Inquiry; however, the ALRC has drafted model UPPs—discussed in detail in Part D—to serve as a guide for the Office of Parliamentary Counsel, which ultimately will have the task of redrafting the *Privacy Act* in accordance with those recommendations accepted by Government.

---

102 The ALRC has a strong record of having its advice followed. About 59% of the ALRC's previous reports have been fully or substantially implemented, about 29% of reports have been partially implemented, 4% of reports are under consideration and 8% have had no implementation to date.

2. Privacy Regulation in Australia

Contents

Introduction

2.1 In this chapter, the ALRC provides an overview of the regulation of personal information in Australia. First, the chapter discusses the constitutional framework for privacy laws in Australia and federal privacy legislation. The chapter then outlines the saving of state and territory privacy laws by the *Privacy Act 1988* (Cth) and the regulation of privacy by the states and territories. The final section considers other forms of privacy regulation such as rules, codes and non-binding guidance.[1]

1 In Ch 4, the ALRC sets out its approach to privacy regulation in Australia. The ALRC recommends a hybrid regulatory model that draws heavily on principles-based and compliance-oriented regimes. A pure principles-based regime will not always meet the objectives of privacy regulation, however, and the ALRC's regulatory model contains a combination of primary legislation, regulations and other legislative instruments, and non-binding guidance.

Federal regulation of privacy

The *Australian Constitution* and privacy

2.2 The *Australian Constitution* establishes a federal system of government in which powers are distributed between the Commonwealth and the six states. It includes a list of subjects about which the Australian Parliament may make laws. That list does not include privacy expressly but this does not mean that the Australian Parliament has no power in relation to privacy.

2.3 The principal piece of federal legislation regulating privacy in Australia is the *Privacy Act*. The *Privacy Act* was passed partially in reliance on the basis of the Australian Parliament's express power to make laws with respect to 'external affairs'.[2] The external affairs power enables the Australian Parliament to make laws with respect to matters physically external to Australia;[3] and matters relating to Australia's obligations under bona fide international treaties or agreements, or customary international law.[4] The external affairs power is not confined to meeting international obligations, but also extends to 'matters of international concern'.[5]

2.4 The Preamble to the *Privacy Act* makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the United Nations *International Covenant on Civil and Political Rights* (ICCPR)[6] and the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines).[7] The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, though this instrument does not, of course, bind Australia.[8] In Chapter 3, the ALRC discusses further the Australian Parliament's power under the *Australian Constitution* to enact federal privacy laws.

Privacy Act 1988 (Cth)

2.5 The *Privacy Act* regulates the handling of personal information by the Australian Government, the ACT Government and the private sector. The Act contains

---

2 *Australian Constitution* s 51(xxix). See *Privacy Act 1988* (Cth) Preamble.

3 *Horta v Commonwealth* (1994) 181 CLR 183.

4 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Polyukhovich v Commonwealth* (1991) 172 CLR 501; *Horta v Commonwealth* (1994) 181 CLR 183.

5 *Koowarta v Bjelke-Petersen* (1982) 153 CLR 168.

6 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17. See discussion in Ch 3.

7 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed further in Part D. Section 3 of the *Privacy Amendment (Private Sector) Act 2000* (Cth) makes clear that the private sector amendments were also intended to meet Australia's international obligations, as well as international concerns, relating to privacy.

8 *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).

a set of 11 Information Privacy Principles (IPPs) that apply to Australian Government and ACT Government agencies, and 10 National Privacy Principles (NPPs) that apply to the private sector. In Chapter 5, the ALRC provides an overview of the *Privacy Act*.

2.6 The *Privacy Act* does not regulate the handling of personal information by the state governments or the Northern Territory Government, except to a very limited extent. The *Privacy Act* is expressed to bind the Crown 'in right of the Commonwealth, of each of the States, of the Australian Capital Territory, of the Northern Territory and of Norfolk Island'.[9] State and territory public sector 'authorities', however, fall outside the definition of public sector 'agency', and are specifically excluded from the definition of private sector 'organisation'.[10] State and territory authorities include ministers, departments, bodies established or appointed for a public purpose under state and territory law, and state and territory courts.[11] Under s 6F of the *Privacy Act*, however, states and territories may request that state and territory authorities be brought into the regime by regulations made under the Act.[12]

Other relevant federal legislation

2.7 Other federal legislation also regulates the handling of personal information. For example, the *Freedom of Information Act 1982* (Cth) (FOI Act) provides that every person has a right of access to documents held by government agencies or ministers, other than exempt documents. A document is exempt from the freedom of information regime if its disclosure would involve unreasonable disclosure of 'personal information'.[13] This exemption is subject to an exception that a person cannot be denied access to a document on the basis that it contains his or her own personal information.[14] The *Archives Act 1983* (Cth) provides a similar exemption.[15]

2.8 The handling of tax file numbers (TFNs) is regulated under various federal Acts, including the *Income Tax Assessment Act 1936* (Cth) and the *Taxation Administration Act 1953* (Cth). The *Data-matching Program (Assistance and Tax) Act 1990* (Cth) regulates data-matching using TFNs.

2.9 Various provisions under other federal legislation require or authorise certain acts and practices, including the collection, use and disclosure of personal information.

---

9 *Privacy Act 1988* (Cth) s 4.
10 Ibid s 6C(1).
11 Ibid s 6C(3).
12 Ibid s 6F. Only four state authorities have been brought into the regime by regulation. This issue is discussed in detail in Ch 38. In 1994, as part of the transition to self-government, the ACT public service was established as a separate entity from the Australian Government public service. The *Privacy Act* was amended at that time to ensure that ACT public sector authorities continued to be covered by the Act: *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).
13 *Freedom of Information Act 1982* (Cth) s 41.
14 Ibid s 41(2).
15 *Archives Act 1983* (Cth) s 33. See discussion in Ch 15.

For example, the *Census and Statistics Act 1905* (Cth) and the *Commonwealth Electoral Act 1918* (Cth) require or authorise the collection of large amounts of personal information. Other Acts require or authorise the disclosure of personal information in a range of circumstances, such as the *Australian Passports Act 200*5 (Cth), *Corporations Act 2001* (Cth), *Telecommunications Act 1997* (Cth), *Telecommunications (Interception and Access) Act 1979* (Cth) and *Migration Act 1958* (Cth). Federal legislation also contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office. Federal legislation that regulates the handling of personal information is discussed in detail in Chapters 15 and 16.

State and territory regulation of privacy

2.10 Each Australian state and territory regulates the management of personal information. In some states and territories, personal information is regulated by legislative schemes, in others by administrative regimes.

2.11 Section 3 of the *Privacy Act* states:

> It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.

2.12 The provision makes clear that the Australian Parliament did not intend to 'cover the field' and to override state and territory laws relating to the protection of personal information if such laws are capable of operating alongside the *Privacy Act*. Section 3 of the *Privacy Act* is discussed in Chapter 3.

2.13 New South Wales (NSW), Victoria and the ACT all have legislation that regulates the handling of personal health information in the private sector. This means that health service providers and others in the private sector in those jurisdictions are required to comply with both federal and state or territory legislation in relation to personal health information. Part H of this Report discusses the issues and problems inherent in this situation. Methods for dealing with these issues are outlined in Chapter 3.

New South Wales

Privacy and Personal Information Protection Act 1998 (NSW)

2.14 NSW was the first state to enact public sector privacy laws. The *Privacy and Personal Information Protection Act 1998* (NSW) contains a set of privacy standards

called Information Protection Principles that regulate the way NSW public sector agencies handle personal information (excluding health information).[16]

2.15 A number of the Information Protection Principles are similar to the IPPs in the *Privacy Act*, but they are not identical.[17] There are four major sources of exemptions to the *Privacy and Personal Information Protection Act*: in the Act;[18] in regulations;[19] in a privacy code of practice, made by the Attorney General;[20] and in a public interest direction made by the NSW Privacy Commissioner.[21]

2.16 The Act provides for the development of privacy codes of practice. A privacy code may modify the application to any public sector agency of one or more of the Information Protection Principles[22] and may exempt a public sector agency or class of public sector agency from the requirement to comply with any of the Information Protection Principles.[23] The Act also provides for privacy management plans.[24]

2.17 The Act establishes the Office of the NSW Privacy Commissioner (Privacy NSW). The NSW Privacy Commissioner has a number of functions, including a complaint-handling function. The NSW Privacy Commissioner must endeavour to resolve complaints by conciliation[25] and may also make written reports on any findings or recommendations made in relation to a complaint.[26]

2.18 Under the existing privacy regime in NSW, there are two avenues of complaint available to individuals who believe that their privacy has been infringed. The individual may make a complaint directly to Privacy NSW.[27] Alternatively, those who believe that their privacy has been interfered with by a NSW public sector agency can submit a complaint directly to the agency and request that the agency conduct an internal review of the behaviour that led to the complaint. Privacy NSW is responsible

---

16 *Privacy and Personal Information Protection Act 1998* (NSW) s 4A. See the discussion of the *Health Records and Information Privacy Act 2002* (NSW) below.

17 The *Privacy and Personal Information Protection Act 1998* (NSW) 'adopted with few modifications, the same principles as contained in the Federal Privacy Act': Privacy NSW, *Submission to the New South Wales Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998*, 24 June 2004, 17. The *Privacy and Personal Information Protection Act 1998* (NSW) was enacted before the inclusion of the NPPs in the *Privacy Act*.

18 For example, there are exemptions for law enforcement and investigative agencies: *Privacy and Personal Information Protection Act 1998* (NSW) pt 2 div 3.

19 For example, there are exemptions relating to privacy management plans under the *Privacy and Personal Information Protection Regulation 2005* (NSW) regs 5–7.

20 *Privacy and Personal Information Protection Act 1998* (NSW) ss 29–32.

21 Ibid s 41.

22 Ibid s 30(1).

23 Ibid s 30(2).

24 A privacy management plan must include provisions relating to the development of privacy policies and practices by a NSW public sector agency: Ibid s 33.

25 Ibid s 49.

26 Ibid s 50.

27 Ibid pt 4.

for the oversight of internal reviews.[28] If an individual is not satisfied with the finding of the review or the action taken by the agency in relation to the application, the individual may apply to the NSW Administrative Decisions Tribunal for a review of the conduct.[29]

2.19 In 2005–06, 81 complaints were made directly to Privacy NSW.[30] The majority of those complaints were against state government agencies. A significant proportion, however, were also against private organisations and local governments.[31] The most common complaints received by Privacy NSW were about disclosure of information, surveillance and physical privacy, and collection of information.[32] NSW public sector agencies handled 100 complaints as internal reviews, which were then overseen by Privacy NSW.[33]

Health Records and Information Privacy Act 2002 (NSW)

2.20 The *Health Records and Information Privacy Act 2002* (NSW) implements a privacy regime for health information held in the NSW public sector and the private sector (except small businesses as defined in the *Privacy Act*).[34] The Act allows for individuals to obtain access to health information and establishes a framework for the resolution of complaints regarding the handling of health information.[35]

2.21 The Act contains 15 Health Privacy Principles (HPPs) that outline how health information must be collected, stored, used and disclosed. The HPPs can be grouped into seven areas: collection; storage; access and accuracy; use; disclosure; identifiers

---

28 Ibid pt 5.

29 Ibid s 55.

30 This is a significant decrease in the number of complaints received the previous year. In 2004–05, Privacy NSW reported that it received 111 complaints: Privacy NSW, *Annual Report 2004–05* (2005), 29. Privacy NSW provides a number of reasons for the drop in complaints: the general public is becoming more aware of the internal review process and increasingly taking the internal review option rather than requesting an investigation by Privacy NSW; agencies have become increasingly familiar with the provisions of the Act; since October 2004, Privacy NSW has been unable to conduct training sessions (training activities raise the profile of the Office and generate further enquiries and requests for advice from the trainees); it is likely that the number of complaints made to a privacy regulator tends to decrease or plateau a few years after the regulator begins operation; and it is expected that some individuals did not need to contact Privacy NSW because they had obtained the information they needed from the Privacy NSW website: Privacy NSW, *Annual Report 2005–06* (2006), 18.

31 The *Privacy and Personal Information Protection Act 1998* (NSW) applies primarily to the NSW public sector. The NSW Privacy Commissioner has the power, however, to investigate and conciliate privacy breaches by organisations and individuals who are not public sector agencies: *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k), (l). The NSW Privacy Commissioner also has functions under the *Health Records and Information Privacy Act 2002* (NSW), which regulates both the public sector and private sector.

32 Privacy NSW, *Annual Report 2005–06* (2006), 47.

33 Ibid, 47.

34 See definition of 'private sector person' in *Privacy and Personal Information Protection Act 1998* (NSW) s 4. The Act did not commence until 25 September 2004: *New South Wales Government Gazette (Health Records and Information Privacy Act 2002*), 27 August 2004, 6683.

35 *Health Records and Information Privacy Act 2002* (NSW) s 3.

and anonymity; and transferrals and linkage.[36] The Act provides for a number of exemptions from these principles. For example, the Act does not apply to the Independent Commission Against Corruption (ICAC), except in connection with the exercise of its administrative and educative functions.[37] Further, the HPPs themselves include exemptions,[38] some of which are the subject of statutory guidelines.[39]

2.22 The *Health Records and Information Privacy Act* provides two avenues of complaint for individuals. Parts 3 and 6 of the Act allow individuals to make complaints directly to the NSW Privacy Commissioner,[40] or direct their complaints to the NSW public sector agency for internal review of the conduct that lead to the complaint.[41] In 2005–06, Privacy NSW received 28 complaints relating to health records.[42] NSW public sector agencies handled 20 complaints concerning health records as internal reviews, which were then overseen by Privacy NSW.[43]

Other legislation

2.23 The *Workplace Surveillance Act 2005* (NSW) prohibits covert surveillance of employees in the workplace without appropriate notice. Three categories of surveillance are covered: camera surveillance; surveillance of an employee's use of a work computer; and surveillance of the location or movements of an employee.[44]

2.24 The *Surveillance Devices Act 2007* (NSW) was recently enacted to regulate the installation, use, maintenance and retrieval of surveillance devices; restrict the use, publication and communication of information obtained through the use of surveillance devices; and establish procedures for law enforcement officers to obtain warrants or

---

36 Ibid sch 1. The *Health Records and Information Privacy Act 2002* (NSW) was a result of the recommendations of the Ministerial Advisory Committee on Privacy and Health Information. According to the Second Reading Speech the development of the legislation was also guided by three additional principles: obligations already imposed on service providers and health service providers by existing laws, such as the federal *Privacy Act*; drawing together the best elements of existing privacy legislation at a local, national and international level (in particular the obligations imposed under the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records Act 2001* (Vic)); and to ensure a readily accessible and usable set of principles having due regard to both individual rights and the special needs arising in the management and use of health information. Consistency with the federal *Privacy Act* was a particular issue: New South Wales, *Parliamentary Debates*, Legislative Council, 11 June 2002, 2958 (M Egan—Treasurer and Minister for State Development).

37 *Health Records and Information Privacy Act 2002* (NSW) s 17.

38 See, eg, Ibid sch 1, HPP 10(1)(c).

39 See, eg, Privacy NSW, *Health Records and Information Privacy Act 2002 (NSW): Statutory Guidelines on the Management of Health Services* (2004).

40 *Health Records and Information Privacy Act 2002* (NSW) s 58.

41 Ibid pt 3.

42 Privacy NSW, *Annual Report 2005–06* (2006), 47.

43 Ibid, 47.

44 *Workplace Surveillance Act 2005* (NSW) pt 3.

emergency authorisations for the installation, use, maintenance and retrieval of surveillance devices. The Act repeals the *Listening Devices Act 1984* (NSW).[45]

Victoria

Information Privacy Act 2000 (Vic)

2.25 The *Information Privacy Act 2000* (Vic) came into force on 1 September 2002. The Act covers the handling of personal information (except health information) in the state public sector in Victoria, and by other bodies that are declared to be 'organisations' for the purposes of Act.[46] Organisations performing work for the Victorian government may also be subject to the Act, depending on the particular contract.[47]

2.26 The Act requires public sector agencies to comply with 10 Information Privacy Principles or have an approved code of practice.[48] The Information Privacy Principles are similar to the NPPs in the *Privacy Act*.[49] The Act contains a number of exemptions, including in relation to courts and tribunal proceedings, publicly available information and law enforcement.[50]

2.27 The Act establishes the Office of the Victorian Privacy Commissioner (OVPC). The Victorian Privacy Commissioner's functions include the receipt of complaints about an act or practice that may contravene an Information Privacy Principle or that may interfere with the privacy of an individual.[51] The complaint-handling procedure includes a conciliation process and conciliation agreement. The Victorian Privacy Commissioner also has the power to issue compliance notices in order to enforce the Information Privacy Principles.[52] Unlike the federal Privacy Commissioner or the Victorian Health Services Commissioner, the Victorian Privacy Commissioner has no power to decide that a breach of privacy has occurred.

---

45 The Act was assented to on 23 November 2007. The Act commences on a day or days to be appointed by proclamation: *Surveillance Devices Act 2007* (NSW) s 2. At 31 March 2008, the Act was still to be proclaimed.

46 *Information Privacy Act 2000* (Vic) s 9.

47 Ibid s 17.

48 Codes of practice are provided for in Ibid pt 4.

49 Ibid sch 1. 'Some modifications to the National Principles have been made to reflect the responsibilities of public sector organisations to promote public interests and be accountable for the expenditure of public funds … In adapting the National Principles under Victorian law it is intended that as much consistency as possible can be maintained with perceptions and practice already operating nationally': Explanatory Memorandum, Information Privacy Bill 2000 (Vic), 7.

50 *Information Privacy Act 2000* (Vic) pt 2 div 2.

51 Ibid s 58.

52 Ibid s 44.

2.28 The OVPC received 54 new complaints in 2006–07.[53] The most common complaints were against state government departments (18 complaints), local councils (11 complaints), law enforcement bodies (nine complaints) and against statutory authorities (seven complaints). Complaints related to use and disclosure, data security and the collection of information.[54]

Health Records Act 2001 (Vic)

2.29 The *Health Records Act 2001* (Vic) covers the handling of all health information held by health service providers in the state public sector[55] and the private health sector.[56] The Act contains 11 Health Privacy Principles adapted from the NPPs in the *Privacy Act*.[57] The Act contains a few exemptions to these principles, including for: dealing with health information for personal, family or household affairs; publicly available health information; and the news media.[58]

2.30 The Act is administered by the Office of the Health Services Commissioner, which may receive complaints about an act or practice that may be an interference with the privacy of the complainant.[59] The Commissioner can deal with a complaint in a number of ways, including by conducting an investigation, by conciliation, a hearing, issuing a compliance notice, or referring a complaint to the Victorian Civil and Administrative Appeals Tribunal.[60] In 2006–07, the Office of the Health Services Commissioner accepted 89 complaints that related to the *Health Records Act*.

2.31 The Health Services Commissioner has the power to issue or approve guidelines. These guidelines may lessen the level of privacy protection afforded by a relevant Health Privacy Principle.[61]

---

53 This is a significant decrease in the number of complaints that were received in the previous year. The OVPC reported that in 2005–06 it received 82 new complaints: Office of the Victorian Privacy Commissioner, *Annual Report 2005–06* (2006), 23. It stated that the 2005–06 complaint numbers were significantly increased by 21 complaints against a single organisation about the same subject matter: Office of the Victorian Privacy Commissioner, *Annual Report 2006–07* (2007), 18.

54 Office of the Victorian Privacy Commissioner, *Annual Report 2006–07* (2007), 18–20.

55 *Health Records Act 2001* (Vic) s 10.

56 Ibid s 11.

57 'The core elements of the HPPs are consistent with the Information Privacy Principles in Schedule 1 of the *Information Privacy Act 2000*. However, the HPPs specifically address issues pertaining to health information and the provision of health services, and adjusted to have appropriate application to both the public and private sectors': Explanatory Memorandum, Health Records Act 2001 (Vic), 6. *The Health Records Act 2001* (Vic) was designed to operate concurrently with any relevant Commonwealth laws: Victoria, *Parliamentary Debates*, Legislative Assembly, 23 November 2000, 1906 (J Thwaites—Minister for Health).

58 *Health Records Act 2001* (Vic) pt 2 div 3.

59 Ibid s 45.

60 Ibid pt 6.

61 Ibid pt 4.

Workplace privacy

2.32 In October 2005, the Victorian Law Reform Commission (VLRC) released *Workplace Privacy—Final Report* (2005).[62] The VLRC concluded that significant legislative gaps in the protection of privacy in workplaces required regulation at the state level, and recommended the enactment of workplace privacy legislation and the establishment of a workplace privacy regulator.[63]

2.33 The Victorian Parliament has enacted the *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).[64] The Act implements the recommendation of the VLRC report that acts or practices of employers which involve installation, use or maintenance of surveillance devices in relation to their workers should be regulated.[65] The Act amends the *Surveillance Devices Act 1999* (Vic) to make it an offence for an employer knowingly to install, use or maintain an optical surveillance device or listening device to observe, listen to, record or monitor the activities or conversations of a worker in workplace toilets, washrooms, change rooms or lactation rooms.[66] There are some limited exceptions to this general prohibition.[67]

2.34 In March 2008, the Standing Committee of Attorneys-General (SCAG) considered options for reform in the area of workplace privacy. SCAG agreed that a minimum model for nationally consistent workplace privacy regulation should be developed. In SCAG's view, such a model should be supported by legislation, and include a combination of measures such as mandatory and voluntary codes of practice. If a jurisdiction imposes a stricter standard than the minimum model, then the stricter standard should continue to apply in that jurisdiction.[68]

Charter of Human Rights and Responsibilities Act 2006 (Vic)

2.35 The *Charter of Human Rights and Responsibilities Act 2006* (Vic) introduced a Charter of Human Rights and Responsibilities for the protection and promotion of human rights in Victoria.[69] Part 2 of the Act sets out a number of human rights including the right of a person not to have unlawful or arbitrary interference with his or her privacy, family, home or correspondence. The Act requires statutory provisions to be interpreted in a way that is compatible with the human rights set out under Part 2 of the Act. It will also require public authorities to act in a way that is compatible with

---

62 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005).

63 Ibid, recs 1–65.

64 The Act commenced on 1 July 2007: *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 2.

65 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), rec 31.

66 *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 3.

67 Surveillance is permitted: in accordance with a warrant or emergency authorisation or a corresponding warrant or emergency authorisation; in accordance with a law of the Commonwealth; or if required by a condition of a liquor licence granted under the *Liquor Control Reform Act 1998* (Vic): *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 3.

68 Standing Committee of Attorneys-General, 'Communiqué' (Press Release, 28 March 2008).

69 The Act, except Divisions 3 (Interpretation of Laws) and 4 (Obligations of Public Authorities) of Part 3, commenced on 1 January 2007. Divisions 3 and 4 of Part 3 commenced on 1 January 2008.

those human rights. The Act is administered by the Victorian Equal Opportunity and Human Rights Commission.

Queensland

2.36 In 1997, the Legal, Constitutional and Administrative Committee of the Queensland Legislative Assembly recommended the enactment of a privacy regime for Queensland based on a set of information privacy principles and the establishment of a Privacy Commissioner.[70] While this recommendation has not been implemented, an administrative scheme was established in 2001, based on the IPPs and the NPPs in the *Privacy Act*. Details of the scheme are provided in Information Standards issued by the Department of Innovation and Information Economy under the *Financial Management Standard 1997* (Qld).[71]

Information Standard 42

2.37 *Information Standard 42—Information Privacy* (IS 42) requires the Queensland state public sector to manage personal information in accordance with a set of Information Privacy Principles adapted from the IPPs in the *Privacy Act*. IS 42 applies to all accountable officers and statutory bodies as defined in the *Financial Administration and Audit Act 1977* (Qld) (including government departments). It also applies to most statutory government-owned corporations.[72]

2.38 The requirement for agencies to comply with IS 42 is administratively based. This means that, where conflicting legislative requirements exist, these will prevail. In addition, compliance is subject to any existing outsourcing arrangements, contracts and licenses.[73] IS 42 provides for two types of exemptions, one concerning exempt bodies; the other relating to personal information.[74]

2.39 IS 42 contains a number of requirements, including that departments and agencies nominate a privacy contact officer; and that they develop, publish and implement privacy plans to give effect to the Information Privacy Principles.[75] IS 42 provides that agencies may develop codes of practice that modify the application of the

---

70 The Committee recognised 'the desirability to have national consistency in privacy protection regimes applicable to both the public and private sectors given the increasingly blurred distinction between those two sectors' and concluded that 'as far as possible, there should be consistency in privacy standards required of the Commonwealth and Queensland public sectors': Legislative Assembly of Queensland—Legal Constitutional and Administrative Review Committee, *Privacy in Queensland*, Report No 9 (1998), [6.1.3].

71 *Financial Management Standard 1997* (Qld) ss 22(2), 56(1).

72 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].

73 Ibid, [1.1].

74 Ibid, [1.2].

75 Ibid, [3.1].

Information Privacy Principles.[76] A set of guidelines has been developed to assist agencies to comply with their obligations in this regard.[77]

2.40 The Queensland Government Department of Justice and Attorney-General is responsible for the administration of privacy in Queensland under IS 42, which includes initiating whole of government privacy initiatives, providing policy advice and dispensing best practice advisory services to Queensland Government agencies and the community.

Health information

Queensland Health Quality and Complaints Commission Act 1992 (Qld)

2.41 In 2006, the *Health Rights Commission Act 1992* (Qld) was repealed by the *Health Quality and Complaints Commission Act 2006* (Qld). The new Act replaces the Health Rights Commission with the Health Quality and Complaints Commission (HQCC). The HQCC is responsible for the oversight of public and private health service delivery in Queensland, and for addressing complaints associated with health service delivery in Queensland. Although there is no specific provision for privacy complaints under the *Health Quality and Complaints Commission Act*, the HQCC reported that in 2006–07 it received 111 complaints related to 'privacy/discrimination' out of a total of 2,832 complaints.[78]

2.42 Chapter 4 of the *Health Quality and Complaints Commission Act* requires the HQCC to develop a Code of Health Rights and Responsibilities.[79] In developing the content of the Code, the Commission must have regard to a number of principles, including that the confidentiality of information about an individual's health should be preserved; an individual is entitled to reasonable access to records about the individual's health; and an individual is entitled to reasonable access to procedures for the redress of grievances relating to the provision of health services.[80]

2.43 The HQCC has released a *Draft Code of Health Rights and Responsibilities* (Draft Code) for consultation.[81] The Draft Code is intended to apply to all health service providers, health service users and their carers throughout the public and private sectors in Queensland.[82]

---

76 Ibid, [1.3].

77 Queensland Government, *Information Standard 42—Information Privacy Guidelines* (2001).

78 Queensland Government Health Quality and Complaints Commission, *Annual Report 2006–07* (2007), 37.

79 *Health Quality and Complaints Commission Act 2006* (Qld) s 31.

80 Ibid ss 33, 34.

81 Queensland Government Health Quality and Complaints Commission, *Draft Code of Health Rights and Responsibilities* (2007). At the time of writing in April 2008, public consultation on the draft code had concluded and the Health Quality and Complaints Commission was preparing a final code for the presentation to the Queensland Minister for Health in 2008.

82 Ibid, 2.

2.44 The Draft Code contains seven statements of health rights. Statement 6 outlines that: 'You have a right to access your personal health information, confidentiality and accurate record keeping'. This statement is broken down into four entitlements of health service users: service provision in a confidential environment; accurate and objective recording of health information; confidential keeping of health information and records; and access to personal information. Each entitlement sets out the responsibilities of providers and users.[83]

Health Services Act 1991 (Qld)

2.45 Part 7 of the *Health Services Act 1991* (Qld) provides that it is an offence for a designated person or former designated person to disclose confidential information that identifies a person who is receiving, or has received, a public sector health service.[84] The provision is subject to a number of exceptions, for example: with consent; where required or permitted by law; to assist in averting a serious risk to life, health or safety, or public safety.[85]

Information Standard 42A

2.46 *Information Standard 42A—Information Privacy for the Queensland Department of Health* (IS 42A) applies only to that Department and requires health information and personal information to be managed in accordance with National Privacy Principles adapted from the NPPs contained in the *Privacy Act*.[86] A number of principles have been deleted as they do not apply to the Queensland Department of Health or are dealt with under other schemes. For example, NPP 6 has been deleted as rights of access and correction are provided for in the *Freedom of Information Act 1992* (Qld).

2.47 IS 42A is similar to IS 42: it contains the same mandatory requirements; similar exemptions; and provides for the development of codes of practice. A set of guidelines has been developed to assist the Department to comply with its obligations under IS 42A.[87]

---

83 Ibid, 9.
84 *Health Services Act 1991* (Qld) s 62A.
85 See Ibid pt 7 div 2.
86 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001).
87 Queensland Government, *Information Standard 42A—Information Privacy Guidelines* (2001).

Other legislation

2.48 The *Invasion of Privacy Act 1971* (Qld) requires the licensing and control of credit reporting agents and regulates the use of listening devices.

Western Australia

2.49 The state public sector in Western Australia does not currently have a legislative privacy regime, although some privacy principles are provided for in the *Freedom of Information Act 1992* (WA). This Act provides for access to documents and the amendment of 'personal information' in a document held by an agency that is inaccurate, incomplete, out-of-date or misleading. The definition of 'personal information' is similar to the definition under the *Privacy Act* except that it also includes information about an individual who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.[88]

2.50 Part 4 of the *Freedom of Information Act 1992* (WA) establishes the Information Commissioner, whose main function is to deal with complaints about decisions made by agencies in respect of access applications and applications for amendment of personal information.[89] The Office of the Information Commissioner received 145 complaints in 2006–07, of which 113 were for external review of a decision under the *Freedom of Information Act 1992* (WA). External review complaints include complaints relating to applications for access to documents and the amendment of personal information under the Act.[90]

2.51 The *State Records Act 2000* (WA) affords some limited protection of privacy. For example, no access is permitted to medical information about a person unless the person consents, or the information is in a form that neither discloses nor would allow the identity of the person to be ascertained.[91] Neither the *State Records Act* nor the *Freedom of Information Act 1992* (WA), however, deal comprehensively with privacy issues associated with the collection, storage and use of personal information by agencies.

---

88 *Freedom of Information Act 1992* (WA) Glossary.

89 Ibid s 63. The Freedom of Information Amendment Bill 2007 (WA) proposes a number of significant amendments to the *Freedom of Information Act 1992* (WA), including: giving the State Administrative Tribunal jurisdiction to deal with complaints on an external review under the FOI Act, and confines the jurisdiction of the Information Commissioner on external review to conciliating complaints; clarifying when an agency may regard an access application as having been withdrawn, and confirming that an agency may delete exempt matter and matter outside the ambit of an access application before providing access to a document; and expanding the functions of the Information Commissioner to include conducting reviews of the internal FOI procedures of an agency.

90 Information Commissioner Western Australia, *Annual Report 2005–06* (2006), 24–25.

91 *State Records Act 2000* (WA) s 49.

Information Privacy Bill 2007

2.52 The Information Privacy Bill 2007 (WA) was introduced into the Western Australian Parliament on 28 March 2007. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information by the public and private sectors in Western Australia.[92] In April 2008, the Bill had been read for a second time in the Legislative Council.

2.53 The Bill requires most state public sector agencies, and contractors to public sector agencies, to comply with a set of eight Information Privacy Principles. The Information Privacy Principles draw heavily on the NPPs contained in the *Privacy Act* and on the Information Privacy Principles in the *Information Privacy Act 2000* (Vic).[93]

2.54 The Bill also requires most public sector agencies, private sector health service providers, and persons or bodies in the private sector who handle health information about individuals, to comply with a set of 10 Health Privacy Principles. The Health Privacy Principles are adapted from, and are consistent with, the *Draft National Health Privacy Code*.[94] They are broadly similar to the general requirements of the NPPs in the *Privacy Act*, but are specifically tailored to the privacy of health information.[95] Under Part 3 Division 2 of the Bill, individuals will be given access to records held by private sector organisations and increased ability to amend their records. This is similar to the power under the *Freedom of Information Act 1992* (WA).

2.55 The Bill contains a number of exemptions, including for courts and tribunals[96] and publicly available information.[97] Some law enforcement agencies and child protection agencies do not have to comply with certain Information Privacy Principles and Health Privacy Principles.[98] The Bill also provides for codes of practice that can derogate from the Information Privacy Principles and the Health Privacy Principles.[99]

---

92 A related Bill, the Freedom of Information Amendment Bill 2007 (WA), was introduced on the same day. This Bill provides the Privacy and Information Commissioner with powers to resolve FOI complaints by conciliation. At the time of writing in April 2008, this Bill also was awaiting passage by the Legislative Council.

93 Western Australia, *Parliamentary Debates*, Legislative Assembly, 28 March 2007 (J McGinty—Attorney General).

94 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003). See Part H for a discussion of the *Draft National Health Privacy Code*.

95 Western Australia, *Parliamentary Debates*, Legislative Assembly, 28 March 2007 (J McGinty—Attorney General).

96 Information Privacy Bill 2007 (WA) cl 9.

97 Ibid cl 10.

98 Ibid cl 11. Sch 2 contains a list of exempt organisations.

99 Ibid cl 15–16, 18–19 and pt 4.

2.56 Part 6 of the Bill overrides prohibitions on the disclosure of personal and health information by public sector agencies, whether those prohibitions result from other statutes, the common law, or ethical or professional obligations, provided the disclosure meets certain criteria. These criteria include, for example, that the disclosure is for the purpose for which the information was collected, or that the disclosure falls within certain specified exceptions to the Information Privacy Principle or Health Privacy Principle relating to use and disclosure.

2.57 The Bill would establish the Privacy and Information Commissioner, who will replace and expand the role of the current Information Commissioner. The Commissioner's functions and powers would include: monitoring and promoting compliance with the Information Privacy Principles and the Health Privacy Principles, reporting to the minister responsible for administering the legislation, and resolving complaints.[100] The complaint-handling process includes the use of conciliation proceedings.[101] Complaints that are not resolved through conciliation may be resolved by the State Administrative Tribunal.[102]

South Australia

Cabinet administrative instruction

2.58 There is no legislation that specifically addresses privacy in South Australia.[103] The South Australian Department of the Premier and Cabinet, however, has issued an administrative instruction requiring its government agencies to comply with a set of Information Privacy Principles based on the IPPs in the *Privacy Act*. *PC012—Information Privacy Principles Instruction* was first issued in July 1989 and then reissued in July 1992.[104]

2.59 The Privacy Committee of South Australia was first established in 1989. In 2001, the Committee was appointed to oversee the implementation of the Information Privacy Principles in the South Australian public sector and to provide advice on privacy issues. The Committee oversees the privacy regime and performs a complaint-handling role. The Committee's functions include the referral of written complaints concerning violations of individual privacy received by it to an appropriate authority.[105] The Committee must prepare a report of its activities annually and submit the report to the minister (currently the Minister for Finance). Members of the public

---

100 Ibid cl 120.

101 Ibid cl 79.

102 Ibid cl 85.

103 There have been recent calls for the introduction of privacy legislation in South Australia. See, eg, 'Democrats Want SA Privacy Commissioner', *ABC News* (online), 6 June 2007, <www.abc.net.au/news>.

104 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

105 Ibid, Sch. The Committee has reported that in 2006–07 it received three new complaints in addition to three existing complaints. The Committee concluded three of the six complaints: Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2006–07* (2007), [3.6].

who are unsatisfied with the Privacy Committee's response to their complaint are referred to the South Australian Ombudsman for further investigation.[106] The Committee is also able to exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit.[107]

2.60 The ALRC has been informed that State Records of South Australia (State Records), in supporting the Privacy Committee of South Australia, is developing a guideline for matching and sharing personal information. State Records is also examining other opportunities for guidelines and proposed amendments to the Instruction that might improve the protection of privacy within the South Australian public sector. Other projects include the development of a standard under the *State Records Act 1997* (SA) relating to contracting out and the handling of personal information.[108]

Code of Fair Information Practice

2.61 South Australia also has a *Code of Fair Information Practice* based on the NPPs in the *Privacy Act*.[109] The Code applies to the South Australian Department of Health and the Department for Families and Communities.[110]

Tasmania

Personal Information Protection Act 2004 (Tas)

2.62 The *Personal Information Protection Act 2004* (Tas) regulates the collection, use and disclosure of personal information. The Act applies to 'personal information

---

106 Privacy Committee of South Australia, *Privacy Committee Members' Handbook Version 1.1* (2005), 16.

107 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992), sch; Privacy Committee of South Australia, *Privacy Committee Members' Handbook Version 1.1* (2005), App 1. The Committee granted three exemptions in 2006–07: Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2006–07* (2007), [3.7].

108 State Records of South Australia, *Correspondence*, 13 June 2007. See also Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2005–06* (2006), [3.4.1], [3.4.2]; Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2006–07* (2007)), [3.3.1].

109 South Australian Government Department of Health, *Code of Fair Information Practice* (2004), Foreword. The Information Privacy Principles are set out in Appendix B. The South Australia Department of Health considered that the NPPs, provided an ideal basis for the Code because 'they are generally applicable to the private sector, particularly those organisations which collect, use, store or disclose "sensitive information"—much of the type of data held by the Department of Health and its service providers'. In adopting the NPPs the South Australia Department of Health was attempting to align 'as much as possible to what looks likely to be the model for a nationally consistent scheme for managing personal information': South Australian Government Department of Health, *Code of Fair Information Practice* (2004), 6.

110 South Australian Government Department of Health, *Code of Fair Information Practice* (2004), 7; Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2004–05* (2005), [3.3.1]; Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2006–07* (2007), [3.7].

custodians' including state government agencies, statutory boards, local councils, the University of Tasmania and any body, organisation or person who has entered into a personal information contract with government agencies relating to personal information.[111] A 'personal information contract' is a contract between a personal information custodian and another person relating to the collection, use or storage of personal information.[112]

2.63 The 10 'Personal Information Protection Principles' set out in Schedule 1 of the Act are based on the NPPs in the *Privacy Act*. Aspects of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Information Privacy Act 2000* (Vic) also have been incorporated into the principles.

2.64 The Tasmanian regime is similar to legislation in other jurisdictions in that it contains exemptions for information concerning law enforcement or that is publicly available.[113] The obligations in relation to 'employee information', however, are different from the federal and other state and territory regimes, in that they allow job applicants and employees to benefit from the privacy obligations imposed on employers.[114] A personal information custodian also may apply to the Minister for Justice for an exemption from compliance with any or all of the provisions of the Act.[115]

2.65 Part 4 of the Act provides for complaints and investigations. Rather than establishing a central body (such as a Privacy Commissioner) to manage complaints, the Tasmanian Ombudsman either investigates and determines the complaint or refers the complaint to another person, body or authority that the Ombudsman considers appropriate in the circumstances.[116] If, on completion of an investigation of a complaint, the Ombudsman is of the opinion that a personal information custodian has contravened a personal information protection principle, the Ombudsman may make any recommendations the Ombudsman considers appropriate in relation to the subject matter of the complaint.[117]

Charter of Health Rights and Responsibilities

2.66 The *Health Complaints Act 1995* (Tas) requires the Health Complaints Commissioner to develop a Charter of Health Rights.[118] The *Charter of Health Rights and Responsibilities* was developed and tabled in Parliament in 1999.

---

111 See definition of 'personal information custodian': *Personal Information Protection Act 2004* (Tas) s 3.
112 Ibid s 3.
113 Ibid ss 8, 9.
114 Ibid s 10.
115 Ibid s 13.
116 Ibid s 20. The Tasmanian Ombudsman reported that in 2006–07 there was no activity under the *Personal Information Protection Act 2004* (Tas): Tasmanian Ombudsman, *Annual Report 2006–2007* (2007), 4.
117 *Personal Information Protection Act 2004* (Tas) s 22.
118 *Health Complaints Act 1995* (Tas) s 17.

2.67 The Charter applies to a wide range of health service providers and provides for six rights, including the right to confidentiality, privacy and security.[119] It sets out a range of rights of health service consumers including the right of a consumer: to have his or her personal health information and any matters of a sensitive nature kept confidential; for health service facilities to ensure his or her privacy when receiving health care; and to expect that information about his or her health is kept securely and cannot easily be accessed by unauthorised persons. The Charter also provides that health service providers have the right to discuss the health care and treatment of a consumer with other providers for advice and support, if it is in the best interest of the consumer's health and wellbeing.[120]

2.68 The Charter is administered by the Health Complaints Commissioner,[121] who has a number of functions including to receive, assess and resolve complaints.[122] Complaints may be resolved by conciliation and through the use of enforceable agreements between a complainant and health service provider.[123] In 2006–07, the Commissioner reported the resolution of 21 privacy-related complaints out of a total of 485 complaints resolved in that period.[124]

Australian Capital Territory

2.69 The ACT public sector complies with an amended version of the *Privacy Act*.[125] The Office of the Privacy Commissioner (OPC) administers the Act on behalf of the ACT government.

Health Records (Privacy and Access) Act 1997 (ACT)

2.70 The *Health Records (Privacy and Access) Act 1997* (ACT) removes health records from the jurisdiction of the OPC. The Act regulates the handling of health records held in the public sector in the ACT and also applies to acts or practices of the

119 Tasmanian Government Office of the Health Complaints Commissioner, *Tasmanian Charter of Health Rights and Responsibilities* (2006), 7.

120 Ibid, 7.

121 In Tasmania, the same person holds the office of the Ombudsman and the Health Complaints Commissioner.

122 *Health Complaints Act 1995* (Tas) s 6(d) and pt 4.

123 Ibid pt 5.

124 Tasmanian Government Health Complaints Commissioner, *Annual Report 2006–07* (2007), 46. The category 'Privacy' includes assault, breach of confidentiality, discrimination, failure to ensure privacy, inconsiderate service and unprofessional conduct. In 2005–06, the Commissioner reported that he resolved 38 privacy-related complaints out of a total of 663 complaints resolved in that period: Tasmanian Government Health Complaints Commissioner, *Annual Report 2005–06* (2006), 52.

125 See *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth). For example, the amended version provides that certain reports following the investigation of a complaint by the Privacy Commissioner are to be supplied to the ACT Attorney-General.

private sector. The Act contains 14 privacy principles that have been modified to suit the requirements of health records.[126]

2.71 The Act gives people access to their own health records or any other record to the extent that it contains personal health information.[127] The Act imposes obligations on both the person requesting access to a health record[128] and the person who responds to a request for access.[129] The Act contains a number of exemptions to the general right of access to health records. For example, it is a ground of 'non-production' if the record or part of the record does not relate in any respect to the person requesting it.[130]

2.72 The ACT Human Rights Commission administers the Act.[131] Under Part 4, a complaint may be made to the Commissioner on the following grounds: the act or omission contravenes the privacy principles in relation to a consumer; the act or omission is a refusal to give access in accordance with the Act to a health record relating to a consumer; or the act or omission is a refusal by a record keeper of a health record to give access to the health record under the Act.

2.73 The Human Rights Commission commenced operation on 1 November 2006. The Commission is an independent agency established by the *Human Rights Commission Act 2005* (ACT). The Commission brings together the existing functions of the ACT Human Rights Office and the Community and Health Services Complaints Commissioner. The *Health Records (Privacy and Access) Act* was previously administered by the ACT Community and Health Services Complaints Commissioner.[132]

Human Rights Act 2004 (ACT)

2.74 Section 12 of the *Human Rights Act 2004* (ACT) provides that all individuals have the right not to have unlawful or arbitrary interferences with their privacy, family, home or correspondence or have their reputation unlawfully attacked. The Act also imposes a duty of consistent interpretation in respect of other legislation. Under the

126 *Health Records (Privacy and Access) Act 1997* (ACT) s 5 and sch 1.
127 Ibid s 10.
128 Ibid s 12.
129 Ibid s 13.
130 Ibid s 14.
131 Ibid pt 4.
132 The ACT Human Rights Commission, *Annual Report 2006–07* (2007) only records complaints relating to health information for the period when the Community and Health Services Complaints Commissioner was receiving complaints (from 1 July 2006 to 31 October 2006). The ACT Human Rights Commission reports that for the period 1 July 2006 to 31 October 2006, the Community and Health Services Complaints Commissioner received 29 complaints relating to privacy and discrimination. Of these complaints, 26 complaints related to access to health records. In 2005–06, the Community and Health Services Complaints Commissioner received 25 complaints about access to health records, and 10 complaints about disclosure of personal health information: ACT Government Community and Health Services Complaints Commissioner, *Annual Report 2005–06* (2006), 40.

Act, when a court is interpreting an ACT law it must adopt an interpretation 'consistent with human rights' as far as possible.[133]

Northern Territory

Information Act 2002 (NT)

2.75 The Northern Territory has combined its information privacy, freedom of information, and public records laws into a single Act, the *Information Act 2002* (NT). Schedule 2 of the Act contains 10 Information Privacy Principles.[134] The Information Privacy Principles are based on the NPPs in the *Privacy Act*.[135] The Act provides for a number of exemptions to the Information Privacy Principles. For example, the Information Privacy Principles do not apply to publicly available information,[136] or to court or tribunal proceedings.[137]

2.76 The Act also provides for approved codes of practice.[138] A code may specify the manner in which a public sector agency is to apply or comply with one or more of the Information Privacy Principles. A code may also modify an Information Privacy Principle, but only in limited circumstances.[139]

2.77 Part 6 of the Act establishes the Information Commissioner for the Northern Territory. The Information Commissioner may authorise a public sector agency to collect, use or disclose personal information in a manner that would otherwise contravene or be inconsistent with specified Information Privacy Principles.[140] The Commissioner also has the power to issue a notice requiring a public sector organisation to take specified action within a period to ensure that in the future it complies with an IPP or code of practice.[141]

2.78 A person may make a complaint to the Commissioner about a public sector organisation that has collected or handled his or her personal information in a manner that contravenes an Information Privacy Principle, a code of practice or an

---

133 *Human Rights Act 2004* (ACT) s 30(1).

134 The Northern Territory does not have health-specific privacy legislation. In 1997, however, the Territory Health Services issued the *Territory Health Services Information Privacy Code of Conduct*. The Code of Conduct includes 11 principles that are based on the IPPs in the *Privacy Act*. The Code covers personally identifiable health information, data collections, staff records, and commercially sensitive information. The Northern Territory Department of Health and Community Services has not used the Code of Conduct since the enactment of the *Information Act 2002* (NT).

135 Northern Territory, *Parliamentary Debates*, Legislative Assembly, 14 August 2002 (P Toyne—Minister for Justice and Attorney-General).

136 *Information Act 2002* (NT) s 68.

137 Ibid s 69. For other exemptions, see *Information Act 2002* (NT) pt 5 div 2.

138 *Information Act 2002* (NT) ss 72–80.

139 Ibid s 72.

140 Ibid s 81.

141 Ibid s 82.

authorisation; or has otherwise interfered with the person's privacy.[142] The Information Commissioner has the power to conduct a hearing in relation to the complaint and make a number of orders.[143] In 2006–07, the Information Commissioner received three privacy complaints.[144]

Code of Health and Community Rights and Responsibilities

2.79 The Northern Territory does not have health-specific privacy legislation, although the *Code of Health and Community Rights and Responsibilities* (the Code) made under s 104(3) of the *Health and Community Services Complaints Act 1998* (NT) confers a number of rights and responsibilities on all users and providers of health and community services in the Northern Territory.[145] The rights and responsibilities set out in the Code do not override duties set out in Northern Territory or federal legislation.

2.80 Principle 4 of the Code relates to personal information. It provides that people have a right to information about their health, care and treatment. They do not have, however, an automatic right of access to their care or treatment records. Under the Principle, health service providers may prevent health service users from accessing their records where legislation restricts the right to access information, or the provider has reasonable grounds to consider that access to the information would be prejudicial to the user's physical or mental health. The Principle also provides that health service providers have a responsibility to protect the confidentiality and privacy of health service users.

2.81 The Northern Territory Health and Community Services Complaints Commission handles complaints in relation to non-compliance with the Code. Complaints are administered under the *Health and Community Services Complaints Act 1998* (NT). Under that Act, the Commissioner may resolve complaints by conciliation,[146] and may receive complaints from the Information Commissioner.[147] The Health and Community Services Complaints Review Committee may review decisions by the Commissioner.[148] In 2006–07, the Commission reported that it did not receive any complaints relating to access to records and that it received one complaint relating to 'privacy/confidentiality'.[149]

---

142 Ibid s 104.
143 Ibid s 115.
144 Northern Territory Government Office of the Information Commissioner, *Annual Report 2006–07*, 21.
145 Northern Territory Government Health and Community Services Complaints Commission, *Code of Health Rights and Responsibilities*, 1.
146 *Health and Community Services Complaints Act 1998* (NT) pt 6.
147 Ibid s 25A.
148 Ibid pt 9.
149 Northern Territory Government Health and Community Services Complaints Commission, *Ninth Annual Report 2006–2007* (2007), 76. In 2005–06, the Commission reported that it did not receive any complaints relating to access to records, and that it received two complaints relating to 'privacy/confidentiality': Northern Territory Government Health and Community Services Complaints Commission, *Eighth Annual Report 2005–2006* (2006), 68.

Proposed health privacy legislation

2.82 In March 2002, the Northern Territory Department of Health and Community Services released a discussion paper, *Protecting the Privacy of Health Information in the Northern Territory*,[150] which sought views on the need for the development of health-specific privacy protection for the Northern Territory. The legislation proposed by the discussion paper would apply to public sector organisations only, and consisted of three main elements: the protection of the privacy of an individual's health information in both the public and private sectors in the Northern Territory; the establishment of a right for individuals to access their own health information; and the conferral of jurisdiction on the Health and Community Services Complaints Commissioner to oversee the health privacy regime and to handle and resolve complaints.[151] To date, a final report has not been released.

Other relevant state and territory legislation

2.83 Personal information is also regulated under state and territory legislation that is not specifically concerned with the protection of personal information. Examples include legislation that contains secrecy provisions, freedom of information legislation, public records legislation, listening and surveillance devices legislation and telecommunications legislation.

2.84 Legislation in each state and territory includes provisions that place obligations on public sector agencies and individuals in the public sector not to use or disclose certain information. For example, s 9 of the *Public Sector Management Act 1994* (WA) requires all public sector bodies to be 'scrupulous in the use of official information'. Other state and territory legislation includes secrecy provisions. Often these provisions state that the disclosure of certain information is an offence.[152] For example, s 22 of the *Health Administration Act 1982* (NSW) provides that it is an offence to disclose information obtained in connection with the administration of the Act, subject to a number of exceptions.

2.85 Each state and territory has freedom of information legislation that enables the public to obtain access to information held by that state or territory government. The right of access to information is subject to a number of exceptions. Documents affecting personal privacy of third parties will usually be exempt from the access requirements under the Act or will be released only after a consultation process.[153]

---

150 Northern Territory Government Department of Health and Community Services, *Protecting the Privacy of Health Information in the Northern Territory*, Discussion Paper (2002).

151 Ibid, Ch 8.

152 Other examples of secrecy provisions include: *Health Administration Act 1982* (NSW) s 22; *Public Health Act 1991* (NSW) s 75; *Criminal Code 1913* (WA) s 81; *Health Act 1911* (WA) ss 246ZM and 314; *Public Sector Management Act 1995* (SA) s 57; *Public Health Act 1997* (Tas) s 139.

153 *Freedom of Information Act 1989* (NSW) s 31 and sch 1 pt 2 cl 6; *Freedom of Information Act 1982* (Vic) s 33; *Freedom of Information Act 1992* (Qld) s 44; *Freedom of Information Act 1992* (WA) s 32;

Freedom of information legislation also attempts to ensure that records held by government concerning the personal affairs of members of the public are complete, correct, up-to-date and not misleading.[154]

2.86 Public records legislation in each state and territory is intended to ensure the effective management of government records and improved record keeping. The legislation provides for public access to records as well as setting out restrictions on access to certain records. Some state and territory public records legislation restricts access to records that contain personal information.[155]

2.87 Some privacy protection is also provided in state and territory legislation regulating the use of listening and other surveillance devices,[156] and telecommunications interception.[157]

2.88 Various state and territory laws regulate the private sector. For example, s 19 of the *Introduction Agents Act 1997* (Vic) regulates the handling of personal information by introduction agencies about their clients. State and territory public health Acts require health service providers, including private health service providers, to collect and record certain information about health consumers with 'notifiable diseases' such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[158] State and territory adoption laws contain a range of provisions regulating adoption records held by government and private adoption agencies, including providing for retention, disclosure and access to information.[159] State and territory laws that regulate the private sector are discussed further in Chapter 3.

Freedom of Information Act 1991 (SA) s 26; *Freedom of Information Act 1991* (Tas) s 30; *Freedom of Information Act 1989* (ACT) s 41; *Information Act 2002* (NT) s 15.

154 *Freedom of Information Act 1989* (NSW) pt 4; *Freedom of Information Act 1982* (Vic) pt V; *Freedom of Information Act 1992* (Qld) pt 4; *Freedom of Information Act 1992* (WA) pt 3; *Freedom of Information Act 1991* (SA) pt 4; *Freedom of Information Act 1991* (Tas) pt 4; *Freedom of Information Act 1989* (ACT) pt 5; *Information Act 2002* (NT) pt 3.

155 *Public Records Act 1973* (Vic) s 9; *Public Records Act 2002* (Qld) ss 16, 18; *State Records Act 2000* (WA) s 49; *Archives Act 1983* (Tas) s 15.

156 *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 1999* (Vic); *Police Powers and Responsibilities Act 2000* (Qld); *Surveillance Devices Act 1998* (WA); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Police Powers (Surveillance Devices) Act 2006* (Tas) (to be proclaimed); *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NT).

157 *Telecommunications (Interception and Access) (New South Wales) Act 1987* (NSW); *Telecommunications (Interception) (State Provisions) Act 1988* (Vic); *Telecommunications (Interception) Western Australia Act 1996* (WA); *Telecommunications (Interception) Act 1988* (SA); *Telecommunications (Interception) Tasmania Act 1999* (Tas); *Telecommunications (Interception) Northern Territory Act 2001* (NT).

158 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

159 See, eg, *Adoption Act 2000* (NSW) ch 8; *Adoption Act 1984* (Vic) pt VI; *Adoption of Children Act 1964* (Qld) pt 4A; *Adoption Act 1988* (SA) pt 2A, pt 3; *Adoption Act 1994* (WA) pt 4; *Adoption Act 1988* (Tas) pt VI; *Adoption Act 1993* (ACT) pt 5; *Adoption of Children Act 1994* (NT) pt 6.

Other forms of privacy regulation

Legislative rules and codes

2.89 Legislation other than the *Privacy Act* allows for the development of privacy codes or rules.[160] For example, s 112 of the *Telecommunications Act* enables bodies and associations in the telecommunications industry to develop industry codes relating to telecommunications activities. In 2000, the Australian Communications Industry Forum (now Communications Alliance Ltd) released an industry code on calling number display (CND).[161] The Code requires suppliers to provide privacy protections in the supply of calling line identification (CLI) and CND; ensures that suppliers adopt procedures to allow callers to freely enable or block CND to the called party; require suppliers to inform their customers about CLI and CND and the privacy implications of both, and how customers can utilise CND blocking features.[162]

2.90 Another example is codes developed pursuant to s 123 of the *Broadcasting Services Act 1992* (Cth). Under this provision, the industry group responsible for representing various radio and television licensees (that is, commercial, subscription and community broadcasters) must develop a code of practice applicable to that section of the broadcasting industry. Privacy provisions are included in the various broadcasting codes of practice developed by representative industry bodies. In the commercial broadcasting and subscription broadcasting sectors, the privacy provisions relate to news and current affairs programs. In the case of the community broadcasting sector, the privacy provisions relate to all programs. For example, Code of Practice 2 of the Commercial Radio Australia *Codes of Practice & Guidelines* provides that news programs (including news flashes) broadcast by a licensee must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, unless there is a public interest in broadcasting such information.[163]

2.91 As noted above, a number of state and territory privacy laws provide for the making of codes that may derogate from the privacy principles in the primary legislation. The Attorney General of NSW has approved a number of privacy codes of practice that modify the application of the *Privacy and Personal Information Protection Act 1998* (NSW). For example, the *Privacy Code of Practice for Local Government* has the effect of modifying the application of Part 6 of the *Privacy and Personal Information Protection Act 1998* (NSW) (the 'public register' provisions) and

160 For other examples of legislative codes and binding guidelines see Ch 17.

161 The Code has been revised a number of times, most recently in 2007: Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2007).

162 Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2007).

163 Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), 2.1(d).

the application of the 12 Information Protection Principles as they apply to local government.[164]

Non-legislative guidance

2.92 In addition to legislative protection of personal information, organisations will often develop and publish privacy guidance that is not required by legislation.[165] For example, the Australian Commission on Safety and Quality in Health Care is developing a National Patient Charter of Rights.[166] The Charter will include a set of principles, including a principle dealing with privacy, which is intended to provide a consistent basis for the development of specific jurisdictional, disease and health service charters.[167]

2.93 In addition, the private sector provisions of the *Privacy Act* exempt from its ambit acts by media organisations in the course of journalism when the organisation is publicly committed to observing a set of privacy standards.[168] The Australian Press Council (APC) has developed a set of eight privacy standards to regulate the handling of personal information.[169] The Standards relate to the collection, use and disclosure of personal information; quality and security of personal information; anonymity of sources; correction, fairness and balance of media reports; sensitive personal information; and complaint handling. The APC receives and deals with complaints in relation to the Standards.

---

164 See, eg, Privacy NSW, *Privacy Codes of Practice* <www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipcodes> at 1 May 2008.

165 For other examples of non-legislative codes and guidelines see Ch 17.

166 Australian Commission on Safety and Quality in Healthcare, *Draft National Patient Charter of Rights* (2008). The Australian Commission on Safety and Quality in Healthcare conducted public consultations on this draft in early 2008, and expects to release a finalised Charter in July 2008.

167 Australian Commission on Safety and Quality in Healthcare, *Draft National Patient Charter of Rights* (2008), 2.

168 *Privacy Act 1988* (Cth) s 7B(4).

169 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 1 May 2008. The Standards adopt the *Privacy Act* definition of 'personal information' and are discussed in more detail in Ch 42.

Commonwealth:

- *Privacy Act 1988*
  - ❑ handling of personal info by Cth & ACT public sector agencies
  - ❑ handling of personal info by some private sector organisations
  - ❑ Part IIIA: credit worthiness info held by credit reporters & providers
  - ❑ tax file number use by individuals & organisations
- *Taxation Administration Act 1953* (handling of tax file numbers)
- *National Health Act 1953* (handling of Medicare and pharmaceutical benefits info)
- *Data-matching Program (Assistance and Tax) Act 1990* (matching b/w ATO & other assistance agencies)
- *Freedom of Information Act 1982*
- *Archives Act 1983*
- *Crimes Act 1914*, Pt VIIC (spent convictions)
- *Surveillance Devices Act 2004*
- *Telecommunications Act 1997* (personal info disclosed by telco providers)
- *Telecommunications (Interception) Act 1979*

* Diagram prepared by the Office of the Victorian Privacy Commissioner, 2007

Northern Territory:

- *Information Act 2002* (privacy, FOI and public records)
- *Surveillance Devices Act 2000*
- *Telecommunications (Interception) Northern Territory Act 2001*

Western Australia:

- No privacy law nor administrative privacy regime, but the Information Privacy Bill 2007 was introduced into Parliament on 28 March 2007
- The *Health Services (Conciliation and Review) Act 1995* (contains guiding principles in relation to health records and patient privacy)
- *Freedom of Information Act 1992*
- *State Records Act 2000*
- *Surveillance Devices Act 1998*
- *Telecommunications (Interception) Western Australia Act 1996*

South Australia:

- No privacy law, but see South Australian Government Department of Premier and Cabinet *PC012–Information Privacy Principles Instruction* (1992)
- *Freedom of Information Act 1991*
- *State Records Act 1997*
- *Criminal Law Consolidation Act 1935*, Part 5A (identity theft)
- *Listening and Surveillance Devices Act 1972*
- *Telecommunications (Interception) Act 1988*

Victoria:

- *Information Privacy Act 2000*
- *Health Records Act 2001*
- *Freedom of Information Act 1982*
- *Public Records Act 1973*
- No spent convictions law, but see Victoria Police, *Information Release Policy* (2007).
- *Charter of Human Rights and Responsibilities Act 2006*
- *Surveillance Devices Act 1999*
- *Telecommunications (Interception) (State Provisions) Act 1988*

Queensland:

- No privacy law, but see: *Information Standard 42—Information Privacy;* and *Information Standard 42A—Information Privacy for the Queensland Department of Health* (administrative standards)
- *Freedom of Information Act 1992*
- *Public Records Act 2000*
- *Invasion of Privacy Act 1971* (credit reporting, listening devices, invasion of privacy of the home)
- *Police Powers and Responsibilities Act 2000* Chap 4 (covert evidence gathering)
- *Health Services Act 1991*
- *Health Quality and Complaints Commission Act 2006*

New South Wales:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *Freedom of Information Act 1989*
- *State Records Act 1998*
- *Surveillance Devices Act 2007* (not yet commenced, but when in operation will repeal *Listening Devices Act 1984*)
- *Workplace Surveillance Act 2005*
- *Telecommunications (Interception and Access) (New South Wales) Act 1987*

Australian Capital Territory:

- *Privacy Act 1988 (Cth)*
- *Health Records (Privacy and Access) Act 1997*
- *Freedom of Information Act 1989*
- *Human Rights Act 2004* (right to privacy)
- *Listening Devices Act 1992*

Tasmania:

- *Personal Information Protection Act 2004*
- *Freedom of Information Act 1991*
- *Archives Act 1983*
- *Listening Devices Act 1991*
- *Telecommunications (Interception) Tasmania Act 1999*
- *Health Complaints Act 1995*

3. Achieving National Consistency

Contents

Introduction

3.1 Australia is yet to achieve uniformity in the regulation of personal information.[1] A key issue raised in recent inquiries[2] and the current ALRC Inquiry,[3] is that

1 In its 1983 report *Privacy* (ALRC 22), the ALRC proposed a national approach to the protection of privacy 'at the very least in relation to information practices': Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1092].

2 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.17]–[4.40] and recs 3, 4; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Ch 2 and recs 2–16; Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), Ch 4 and recs 4.47, 4.48.

3 Inconsistency in the regulation of personal information was raised as an issue in a large number of submissions to the ALRC Inquiry. See, eg, 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; Queensland Government, *Submission PR 490*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See also Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [4.1].

Australian privacy laws are multi-layered, fragmented and inconsistent. For example, the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Cth) (Senate Committee privacy inquiry) concluded that:

> The committee is greatly concerned at the significant level of fragmentation and inconsistency in privacy regulation. This inconsistency occurs across Commonwealth legislation, between Commonwealth and state and territory legislation, and between the public and private sectors. As mentioned above, the committee believes that this inconsistency is one of a number of factors undermining the objectives of the Privacy Act and adversely impacting on government, business, and mostly importantly, the protection of Australians' privacy.[4]

3.2 The various problems caused by inconsistency and fragmentation are outlined in Part C of this Report. This chapter first considers whether national consistency should be one of the goals of the regulation of personal information handling. The chapter then outlines various reforms for achieving greater consistency at the federal, state and territory level. These reforms include the amendment of the *Privacy Act* to provide that the Act is intended to apply to the exclusion of the states and territories in relation to the handling of personal information in the private sector; and an intergovernmental agreement that establishes an intergovernmental cooperative scheme. The scheme would provide that the states and territories should enact legislation to regulate the handling of personal information in the state and territory public sectors that adopts key uniform elements, such as a set of uniform privacy principles. The final section of the chapter outlines various methods for achieving national consistency, including codes, joint guidance, and privacy impact statements.

The federal system

3.3 The *Australian Constitution* establishes a federal system of government in which legislative powers are distributed between the Commonwealth and the six states. Section 109 of the *Australian Constitution* provides that: 'when a law of a State is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid'. This provision may operate in two ways: it may directly invalidate state law where it is impossible to obey both the state law and the federal law;[5] or it may indirectly invalidate state law where the Australian Parliament's legislative intent is to 'cover the field' in relation to a particular matter.[6]

---

4 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.6].

5 *Australian Boot Trade Employees Federation v Whybrow & Co* (1910) 10 CLR 266; *R v Licensing Court of Brisbane; Ex parte Daniell* (1920) 28 CLR 23.

6 *Clyde Engineering Co Ltd v Cowburn* (1926) 37 CLR 466.

3.4 It has been observed that inconsistency in the regulation of personal information stems largely from the failure of federal law to 'cover the field'.[7] Section 3 of the *Privacy Act* states:

> It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.

3.5 The provision makes clear that the Australian Parliament did not intend to 'cover the field' or to override state and territory laws relating to the protection of personal information, if such laws are capable of operating alongside the *Privacy Act*. Section 3 of the *Privacy Act* does not, however, sit comfortably with s 3 of the *Privacy Amendment (Private Sector) Act 2000* (Cth), which states that one of the objects of the Act is

> to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations.[8]

3.6 A number of the states and territories have enacted privacy legislation regulating the handling of personal information in the state and territory public sectors. These regimes are sometimes inconsistent with the *Privacy Act* and with each other.[9] Further, New South Wales, Victoria and the ACT all have legislation that regulates the handling of personal health information in the public and private sectors. This means that health service providers and others in the private sector in those jurisdictions are required to comply with both federal and state or territory legislation.[10]

3.7 Although the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs) and privacy principles under state and territory privacy legislation are similar, they are not identical. The privacy regimes in some jurisdictions include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs.[11]

3.8 The Office of the Privacy Commissioner (OPC) review of the private sector provisions of the *Privacy Act* (OPC Review) recommended that the Australian

---

7 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.21].

8 *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3(a).

9 See discussion in Chs 2, 17.

10 For further discussion of national consistency in the regulation of health information, see Part H.

11 See discussion in Chs 2, 17.

Government should consider amending s 3 of the *Privacy Act* to remove any ambiguity as to the regulatory intent of the private sector provisions.[12]

Is national consistency important?

3.9 A threshold issue is whether national consistency in the regulation of personal information handling is important. All submissions that addressed this issue strongly supported national consistency.[13] Most focused on how a nationally consistent privacy regime would lessen unjustified compliance burdens and cost. For example, a number of stakeholders emphasised that national consistency is essential to lessen the compliance burden for organisations and agencies that operate across state borders.[14] Others argued that the use of technologies—such as the internet—justifies a harmonised approach to privacy regulation at a national and international level.[15]

3.10 A large number of stakeholders identified that state and territory legislation regulating the handling of personal information in the private sector is a major cause of inconsistency, complexity and costs.[16] In particular, stakeholders submitted that inconsistency in the regulation of health information is creating a number of problems, including a significant compliance burden and cost, and preventing projects that are in

---

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

13 See 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; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 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; 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; Queensland Government, *Submission PR 490*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; AXA, *Submission PR 442*, 10 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007. See also Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [4.11].

14 See, eg, Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; CrimTrac, *Submission PR 158*, 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Victorian Society for Computers and the Law Inc, *Submission PR 137*, 22 January 2007; National Association for Information Destruction, *Submission PR 133*, 19 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

15 Microsoft Australia, *Submission PR 113*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

16 See, eg, Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007; Cancer Council Victoria, *Consultation PC 75*, Melbourne, 5 February 2007.

the public interest, such as medical research.[17] These problems arise, in part, because the handling of health information in the private sector is regulated by the *Privacy Act* and state and territory legislation in NSW, Victoria and the ACT.[18]

3.11 Some stakeholders noted, however, that while national consistency is a valuable objective, it should not be pursued to the detriment of the level of protection afforded by privacy legislation.[19] The OPC submitted that:

> Consistency does not mean the elimination of multi-layered regulation. In many cases, additional protections that regulate particular sectors, or protect certain information, can enhance privacy (such as privacy codes and secrecy provisions). However, in the interests of all parties, it is critical to ensure these layers are not unnecessary, inconsistent, or poorly interactive.[20]

3.12 State governments and others maintained that the states and territories should be left to regulate the handling of personal information in their own public sectors. These stakeholders emphasised the benefits of having different levels of government to innovate or respond to local conditions;[21] the need for privacy legislation to interact with other state and territory legislation, such as freedom of information and human rights legislation;[22] and the advantages of having a local regulator to handle complaints and provide advice and training programs.[23]

ALRC's view

3.13 Inconsistency and fragmentation in privacy regulation causes a number of problems, including unjustified compliance burden and cost, impediments to information sharing and national initiatives, and confusion about who to approach to make a privacy complaint. National consistency, therefore, should be one of the goals of privacy regulation.[24] This finding is consistent with the Senate Committee privacy

---

17 See, eg, National Health and Medical Research Council, *Submission PR 114*, 15 January 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Telstra, *Submission PR 185*, 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; Australasian Compliance Institute, *Submission PR 102*, 15 January 2007.

18 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

19 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

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

21 Government of South Australia, *Submission PR 187*, 12 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

22 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

23 Queensland Government, *Submission PR 242*, 15 March 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

24 Professor Fred Cate has stated that individuals should enjoy privacy protection that is as consistent as possible across types of data, settings, and jurisdictions: F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341.

inquiry and the OPC Review, which both concluded that privacy laws should aim to be consistent across Australia.[25]

3.14 The goal of national consistency can be achieved in a number of different ways, including:

- the adoption of uniform privacy principles, any relevant regulations that modify the application of the Unified Privacy Principles (UPPs) and relevant definitions used in the *Privacy Act* at the federal, state and territory level;[26]
- the harmonisation of the *Privacy Act* and other laws that regulate the handling of personal information;[27]
- cooperation and coordination between privacy regulators;[28] and
- consistency in the coverage of privacy laws—for example, the removal of the small business and the employee records exemptions.[29]

3.15 A nationally consistent privacy regime will ensure that Australians' personal information will attract similar protection whether that personal information is being handled by an Australian Government agency or a state or territory government agency, a multinational organisation or a small business, and whether that information is recorded in a paper file or electronically. Ensuring national consistency also will assist:

- individuals to determine what their rights are and how to enforce them;
- agencies and organisations to understand their obligations and how to comply effectively and efficiently with them; and
- regulators in managing the possible overlap of functions in some areas.[30]

3.16 The ALRC is also mindful, however, of the need for flexibility in some areas. A number of stakeholders noted that consistency of information privacy regulation across jurisdictions, between the public and private sectors, and between different kinds of business, can only be achieved if the regulation is flexible enough to accommodate the different interests, business practices, and accountability of those subject to the

---

25 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 3; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 2–7.

26 See below and Ch 17.

27 See, eg, Chs 15, 16.

28 See, eg, Chs 14, 17, 49, 71.

29 See Part E.

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

regulation.[31] Some sectors require specific laws when dealing with personal information, for example, the health sector, credit reporting industry and the telecommunications industry.[32]

Constitutional issues

3.17 This section will examine the scope of the Commonwealth's constitutional power to legislate with respect to privacy, and particularly its constitutional capacity to 'cover the field' in this area.

3.18 The *Australian Constitution* includes a list of subjects about which the Australian Parliament may make laws. That list does not expressly include privacy, but this does not mean that the Australian Parliament has no power in relation to privacy.

3.19 The *Privacy Act* was enacted on the basis of the Australian Parliament's express power to make laws with respect to 'external affairs'.[33] The external affairs power enables the Australian Parliament to make laws with respect to matters physically external to Australia;[34] and matters relating to Australia's obligations under bona fide international treaties or agreements, or customary international law.[35] The external affairs power is not confined to meeting international obligations, but may also extend to 'matters of international concern'.[36]

3.20 An important limitation on the scope of the external affairs power is that the Commonwealth Act must be an appropriate means of giving effect to the object of the relevant international treaty or agreement.[37] The Preamble to the *Privacy Act* makes it

---

31 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007. See also, Centre for Law and Genetics, *Submission PR 127*, 16 January 2007 in relation to health information; and AAPT Ltd, *Submission PR 87*, 15 January 2007 in relation to telecommunications.

32 See Part G, Part H, Part J. See also the ALRC's recommendations in relation to small business in Ch 39.

33 *Australian Constitution* s 51(xxix). See *Privacy Act 1988* (Cth) Preamble.

34 *Horta v Commonwealth* (1994) 181 CLR 183.

35 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Polyukhovich v Commonwealth* (1991) 172 CLR 501; *Horta v Commonwealth* (1994) 181 CLR 183.

36 In *XYZ v The Commonwealth* (2006) 227 CLR 532, the High Court stated that it was unnecessary to decide whether the Australian Parliament may make laws with respect to matters of 'international concern' because the Commonwealth could rely on other recognised aspects of the external affairs power to uphold the validity of the legislation under challenge. Kirby J, however, considered the concept of 'international concern' and concluded that the concept is still 'undeveloped in Australia': Ibid, [125]–[127]. Callinan and Heydon JJ, in dissent, also considered the concept of 'international concern'. In their view, there is no case in the High Court deciding that the 'international concern' doctrine exists. They stated that there 'are dicta which support the view, or which some contend support the view, that it does. But there is less to these dicta than meets the eye': Ibid, [217].

37 *R v Burgess*; *Ex parte Henry* (1936) 55 CLR 608, 646; *R v Poole*; *Ex Parte Henry* (No 20) (1939) 61 CLR 364; *Airlines of New South Wales v New South Wales (No 2)* (1965) 113 CLR 54, 82, 102, 118, 126, 141; *Commonwealth v Tasmania* (1983) 158 CLR 1; *Richardson v Forestry Commission* (1988) 164 CLR

clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the United Nations *International Convention on Civil and Political Rights* (ICCPR)[38] as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines).[39] The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.[40] Section 3 of the *Privacy Amendment (Private Sector) Act* makes clear that the private sector amendments were also intended to meet Australia's international obligations relating to privacy.

3.21 In addition to the 'external affairs' power, the Commonwealth may rely on other constitutional heads of power as a basis for legislating on privacy,[41] including: s 51(v), which empowers the Australian Parliament to make laws with respect to 'postal, telegraphic, telephonic, and other like services';[42] s 51(i), which empowers the Australian Parliament to make laws with respect to 'trade and commerce with other countries, and among the States'; ss 51(xiii) and (xiv), which empower the Australian Parliament to make laws with respect to banking and insurance,[43] but not state banking or state insurance unless it extends beyond the limits of the state; and s 51(xx), which empowers the Australian Parliament to make laws with respect to 'foreign corporations, and trading or financial corporations formed within the limits of the Commonwealth'.[44]

3.22 The Commonwealth may legislate so as to 'cover the field' (either expressly or impliedly) of a particular subject matter within its legislative powers.[45] The Australian Parliament could pass legislation regulating the handling of personal information to the exclusion of the states and territories. Such legislation, however, would be affected by

---

261. There remains legislative discretion to choose among appropriate means for implementing those obligations: *Commonwealth v Tasmania* (1983) 158 CLR 1, 130–131.

38 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

39 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed further in Ch 1 and Part D.

40 *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).

41 Recent human rights legislation has been based on a range of constitutional powers. See, eg, *Age Discrimination Act 2004* (Cth) s 10.

42 For example, pt IIIA of the *Privacy Act* seeks to engage s 51(v) by regulating the use of 'eligible communications services' in the course of activities relevant to credit reporting. The term 'eligible communications services' is defined to mean 'a postal, telegraphic, telephonic or other like service, within the meaning of paragraph 51(v) of the *Constitution*': *Privacy Act 1988* (Cth) s 6(1).

43 This restriction is reflected in s 12A of the *Privacy Act* and is discussed further below.

44 The *Privacy Act* is partly directed towards the actions of 'organisations' in respect of an individual's personal information. 'Organisation' is defined to include 'a body corporate': *Privacy Act 1988* (Cth) s 6C.

45 *Botany Municipal Council v Federal Airports Corporation* (1992) 175 CLR 453, 464–465.

the express and implied restrictions applying to all Commonwealth constitutional powers, discussed below.

Express and implied constitutional limits

3.23 Express constitutional limitations include those in ss 51(xiii) and 51(xiv) of the *Australian Constitution*, which provide that the Australian Parliament may legislate with respect to banking and insurance, but not state banking or state insurance that does not extend beyond the limits of the state. 'State banking' for the purposes of s 51(xiii) is the business of banking conducted within a state by a bank owned or controlled by a state.[46] Similarly, 'state insurance' bears its ordinary meaning, referring to an insurance business established and conducted by a state or its authority.[47]

3.24 If the *Privacy Act* were to operate upon state banking or state insurance not extending beyond the limits of the state concerned, it would be constitutionally valid only so long as it could not be characterised as a law with respect to banking.[48] The same rationale and outcome applies with respect to the insurance power.[49]

3.25 Implied constitutional limitations include the principles that a federal law may not discriminate against a state,[50] or prevent a state from continuing to exist and function as an independent unit of the federation.[51] In *Western Australia v The Commonwealth* a majority of the High Court of Australia determined that:

> For constitutional purposes, the relevant question is not whether State powers are effectively restricted or their exercise made more complex or subjected to delaying procedures by the Commonwealth law. The relevant question is whether the Commonwealth law affects what Dixon J [in *Melbourne Corporation v The Commonwealth*] called the 'existence and nature' of the State body politic … A Commonwealth law cannot deprive the State of the personnel, property, goods and services which the State requires to exercise its powers and cannot impede or burden the State in the acquisition of what it so requires.[52]

3.26 While state powers may be 'effectively restricted or their exercise made more complex or subjected to delaying procedures' by the operation and requirements of the

---

46 *Melbourne Corporation v Commonwealth* (1947) 74 CLR 31, 52, 65, 70, 78, 86, 97.

47 *Attorney-General (Victoria) v Andrews* (2007) 233 ALR 389. See also P Lane, *Lane's Commentary on The Australian Constitution* (1997), 215.

48 *Bourke v State Bank of New South Wales* (1990) 170 CLR 276, 290. The Court's decision has been subject to criticism: D Rose, 'Judicial Reasonings & Responsibilities in Constitutional Cases' (1994) 20 *Monash Law Review* 195, 199–200.

49 *Attorney-General (Victoria) v Andrews* (2007) 233 ALR 389.

50 *Melbourne Corporation v Commonwealth* (1947) 74 CLR 31, 78; *Victoria v Commonwealth* (1957) 99 CLR 575; *Queensland Electricity Commission v Commonwealth* (1985) 159 CLR 192; *Western Australia v Commonwealth* (1995) 183 CLR 373.

51 *Melbourne Corporation v Commonwealth* (1947) 74 CLR 31, 78; *Queensland Electricity Commission v Commonwealth* (1985) 159 CLR 192; *Victoria v Commonwealth* (1971) 122 CLR 353; *Re Australian Education Union; Ex parte Victoria* (1995) 184 CLR 188; *Austin v Commonwealth* (2003) 215 CLR 185.

52 *Western Australia v Commonwealth* (1995) 183 CLR 373, 480.

Privacy Act, the Act does not affect the existence and nature of the 'State body politic'.[53] The Commonwealth could legislate to regulate the handling of personal information in the state public and private sectors to the exclusion of the states.[54]

3.27 Legislative provisions applying to public sector employees in the higher levels of state government may be one qualification to the Commonwealth's power to exclude state and territory privacy legislation. The High Court has found that Commonwealth laws that seek to regulate state employees at the 'higher levels of government' (including ministers, ministerial assistants and advisers, heads of departments and judges) may interfere with the existence and nature of a state.[55] Another limitation may be if the *Privacy Act* purported to regulate the handling of information that goes to the core of state government functions, such as cabinet-in-confidence documents and other highly sensitive documents.

3.28 These express and implied constitutional limitations do not apply to the territories because the Australian Parliament has plenary power to legislate in relation to them.[56] Further, Commonwealth legislation regulating the handling of personal information in the private sector to the exclusion of state legislation would not breach either the express or implied restrictions on Commonwealth power.[57]

Options for reform

3.29 The ALRC has considered various options to achieve national consistency in the regulation of personal information handling, including the amendment of the *Privacy Act* to establish a single national privacy law, and the establishment of an intergovernmental cooperative scheme. These options are outlined below.

National legislation

3.30 As noted above, the Commonwealth has the power under the *Australian Constitution* to amend the *Privacy Act* so that it applies to state and territory public sectors, as well as organisations and the federal public sector.

3.31 In many respects, the preferable option would be to amend the *Privacy Act* to regulate all organisations and public sectors. The advantages of a single national law include guaranteed uniformity across the jurisdictions, and fewer regulatory impediments to the operation of national programs and organisations.

---

53 Ibid, 480.

54 A number of pieces of federal human rights legislation, including the *Age Discrimination Act 2004* (Cth), the *Disability Discrimination Act 1992* (Cth) and the *Racial Discrimination Act 1975* (Cth), regulate the activities of state and territory public sector authorities.

55 *Re Australian Education Union*; *Ex parte Victoria* (1995) 184 CLR 188, 233; *Austin v Commonwealth* (2003) 215 CLR 185.

56 *Australian Constitution* s 122.

57 Re *Lee; Ex parte Harper* (1986) 160 CLR 430, 453; *Western Australia v The Commonwealth* (1995) 183 CLR 373, 477.

3.32 Another option is to extend the operation of the *Privacy Act* to cover certain elements of the state and territory public sectors and not others. As noted above, stakeholders have identified that inconsistent health privacy laws are a major cause of compliance burden and cost. One option would be to amend the *Privacy Act* so that it regulates state and territory statutory corporations and other bodies with responsibility for health services and research, such as public hospitals and universities.

3.33 A third option is to amend the *Privacy Act* to provide that the Act is intended to apply to the exclusion of state and territory laws that deal with the handling of personal information by organisations. A large number of submissions to the Inquiry focused on inconsistency in the regulation of personal information handling in the private sector. Under this option, state and territory legislation would continue to regulate the handling of personal information in state and territory public sectors.

Roll back provisions

3.34 National legislation could set out minimum standards for the protection of personal information in state and territory public sectors, but allow for a 'roll back' of those provisions once a state or territory enacts laws that conform to specified federal minimum standards.[58]

3.35 An example of this kind of scheme is s 26(2)(b) of the *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act). That section provides that the Governor-in-Council may, by order, exempt an organisation, activity or class of organisations or activities from the application of the Act if satisfied that legislation of a province that is 'substantially similar' to the PIPED Act applies. Few stakeholders supported this option. The ALRC did not, therefore, propose that a 'roll back' provision should operate generally in relation to state and territory agencies.

3.36 Section 6F of the *Privacy Act* provides for an extension of the Act to cover the handling of personal information by state and territory instrumentalities at the initiative of the states and territories. The Office of the Victorian Privacy Commissioner (OVPC) submitted that s 6F of the *Privacy Act* should be retained in its current form because it maintains control by, and independence of, the states.[59] The ALRC agrees that s 6F is a useful mechanism to bring state and territory bodies under the operation of the *Privacy Act* and should be retained in the Act.

A cooperative scheme

3.37 Another option is to have the *Privacy Act* regulate the private sector and federal public sector, and establish a cooperative scheme to regulate state and territory public

---

58 There are examples of rollback provisions in various federal laws: *Gene Technology Act 2000* (Cth) s 14; *Environment Protection (Sea Dumping) Act 1981* (Cth) s 9.

59 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

sectors. A cooperative scheme has been defined as a scheme in which each participating jurisdiction promulgates legislation to facilitate the application of a standard set of legislative provisions to regulate a matter of common concern.[60]

3.38 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC considered four types of intergovernmental cooperative schemes: referral of power to the Commonwealth; mirror legislation; complementary law regimes; and a combined scheme.[61] These schemes may involve not only mirror or complementary legislation, but the cooperative use of Australian Government or state and territory officials.[62]

Referral of power to the Commonwealth

3.39 Section 51(xxxvii) of the *Australian Constitution* gives the Commonwealth Parliament power to make laws with respect to:

> matters referred to the Parliament of the Commonwealth by the Parliament or Parliaments of any State or States, but so that the law shall extend only to States by whose Parliaments the matter is referred, or which afterwards adopt the law.

3.40 The states have referred a number of matters to the Commonwealth, including corporations and counter-terrorism.[63] While a referral of power by the states would ensure that federal privacy legislation was comprehensive in its coverage and less vulnerable to constitutional challenge, a referral of power is unnecessary to enact national privacy laws. As noted above, the Commonwealth has the power under the *Australian Constitution* to amend the *Privacy Act* so that it applies to the private sector and all public sectors in Australia.[64]

3.41 There was very little support from stakeholders for a referral of power. The New South Wales Law Society submitted that state governments should consider referring

---

60 J Ledda, 'The Drafter's Guide to Cooperative Schemes' (Paper presented at Drafting Forum 2001, Melbourne) cited in M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 3.

61 Ibid, 3.

62 R French, 'Cooperative Federalism in Australia: An Intellectual Resource for Europe' (Institute of Advanced Legal Studies Public Lecture, London, 22 February 2005), 14.

63 See, eg, *Workplace Relations Act 1996* (Cth) pt 21; *Commonwealth Powers (Industrial Relations) Act 1996* (Vic); *Criminal Code Act 1995* (Cth) pt 5.3; *Terrorism (Commonwealth Powers) Act 2003* (Vic). The *Corporations Act* 2001 (Cth) is based, in part, on reference of matters by the states to the Commonwealth. The decision to adopt such references was influenced by a number of successful challenges to the Commonwealth's attempts to develop uniform corporations law: see *R v Hughes* (2000) 171 ALR 155; *Re Wakim; ex parte McNally* (1999) 198 CLR 511. A reference to the Commonwealth would not be required from the ACT, the Northern Territory and Norfolk Island because s 122 of the *Australian Constitution* assigns to the Commonwealth the power to 'make laws for the government' of the territories.

64 In Ch 8, the ALRC recommends extending certain elements of the *Privacy Act* to cover the personal information of deceased individuals. The relevant international human rights instruments, discussed above, are not expressed to apply to deceased individuals and may not, therefore, provide a firm constitutional basis for legislation at the federal level. In order to avoid uncertainty, it may be preferable to seek a referral of power from the states under s 51(xxxvii) of the *Australian Constitution* in relation to the protection of the personal information of deceased individuals.

powers to enable the Australian Parliament to enact a national privacy code.[65] Other stakeholders emphasised, however, the need for states to be able to provide enhanced protection; the need for privacy laws to interact with state-based freedom of information, archives and human rights laws;[66] and the importance of having a local regulator to handle complaints, and provide advice and training programs.[67]

Mirror legislation

3.42 Mirror legislation usually refers to a system where one jurisdiction enacts a law that is then enacted in similar terms by other jurisdictions.[68] Mirror legislation can result in inconsistency, however, both at the time the legislation is enacted and as laws are amended.[69] One option for dealing with this is to have a central body to maintain uniformity.[70]

3.43 An example of mirror legislation is state and territory fair trading legislation based on provisions in the *Trade Practices Act 1974* (Cth). Each Australian state and territory has passed legislation that largely mirrors the consumer protection provisions of Divisions 1 and 1A of Part V of the *Trade Practices Act.*

3.44 A number of stakeholders supported mirror legislation.[71] For example, the Queensland Government submitted that a consistent set of privacy principles binding both public and private sectors should be adopted by each jurisdiction by way of mirror legislation. Each jurisdiction would then be responsible for administering the relevant legislation, for establishing and maintaining complaint resolution mechanisms, undertaking advocacy, education and awareness activities and monitoring the operation of the scheme.[72]

Complementary law scheme

3.45 A complementary applied law scheme involves one jurisdiction (which need not be the Commonwealth) enacting a law on a topic, which is then applied by other

---

65 Law Society of New South Wales, *Submission PR 443,* 10 December 2007. See also M Fenotti, *Submission PR 86,* 15 January 2007.

66 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

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

68 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 4–5.

69 See, eg, 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), [2.28]; Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Ch 1.

70 See, eg, Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Rec 2–1.

71 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 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.

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

jurisdictions.[73] Where the Australian Parliament enacts a law that applies to specified matters within Commonwealth constitutional power, the law will apply in the states as a Commonwealth law to the extent possible. State legislation will apply to the extent that its application is consistent with the application of the Commonwealth law.[74]

> In the perfect applied law regime where a law is promulgated by one jurisdiction and is picked up by other jurisdictions as in force from time to time, there are effective limits (which may be non-legislative) on modification and there is central administration and enforcement of that law, which can be expected to provide a substantial degree of uniformity.[75]

3.46 Uniformity can be reduced, however, if an applied law regime does not involve centralised control over amendments to the legislation. Further, any capacity for the applying state to have control over the text of the legislation can also lead to inconsistency.[76]

3.47 An example of a complementary applied law scheme is the agricultural and veterinary chemicals legislation under the *Agricultural and Veterinary Chemicals Code Act 1994* (Cth). The Australian Parliament enacted the *Agricultural and Veterinary Chemicals Code* to apply to 'participating territories' and with provisions to enable the states to apply the text of the Code as a law of the state. All states and territories have adopted the Code in relevant legislation.

3.48 The *Agricultural and Veterinary Chemicals Code Act* confers regulatory functions on the National Registration Authority for Agricultural and Veterinary Chemicals, establishing it as the national authority responsible for the evaluation, registration and review of agricultural and veterinary chemicals and their control up to their point of sale. The states and territories retain responsibility for control-of-use activities, such as licensing of pest control, operators and aerial spraying. Some states have also enacted legislation relating to the enforcement of the Code. For example, the *Agricultural and Veterinary Chemicals (Control of Use) Act 1995* (Tas) establishes the Agricultural, Silvicultural and Veterinary Chemical Council. The *Competition Code* under the *Trade Practices Act 1974* (Cth) is another example of a complementary applied law scheme.[77]

3.49 A complementary (non-applied) law scheme has been adopted in relation to the classification of films, publications and computer games. Films, publications and computer games are classified under the *Classification (Publications, Films and*

---

73 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 8.
74 Ibid, 9.
75 Ibid, 10.
76 Ibid, 10.
77 See *Trade Practices Act 1974* (Cth) pt XIA.

Computer Games) Act 1995 (Cth) while the controls and penalties are imposed under state and territory legislation.[78]

3.50 In an information privacy context, the governments of Victoria and South Australia supported a complementary cooperative scheme, where the Commonwealth has responsibility for the private sector and the Australian Government, and the states and territories have responsibility for state and territory public sectors.[79] Other stakeholders were opposed to a complementary non-applied scheme, arguing that this model enables a single jurisdiction to prevent changes to the legislation, notwithstanding overwhelming support for change from the public and other jurisdictions' governments.[80]

Combined scheme

3.51 Another model is a scheme that combines mirror legislation and applied law approaches. In this model, some states could enact their own law mirroring federal laws that regulate personal information and other states could apply the Commonwealth law as a law of the state. Examples of this approach include the therapeutic goods and gene technology regulatory schemes.

3.52 The *Gene Technology Act 2000* (Cth) extends to matters within the Commonwealth's power, leaving the states with the option of either applying the federal Act or enacting their own legislation. Both options have been adopted by different states. For example, NSW has opted for the applied law model while Victoria has adopted mirror legislation.[81] Section 26 of the *Gene Technology Act 2000* (Cth) establishes the independent position of the Gene Technology Regulator. The Regulator oversees the accreditation of research facilities and licenses experimental and commercial dealings.[82]

National legislation to regulate the private sector

'Covering the field'

3.53 In DP 72, the ALRC expressed the view that many of the problems associated with inconsistent privacy laws would be dealt with effectively if the *Privacy Act* was amended to 'cover the field' in relation to the handling of personal information in the

---

78 See, eg, *Classification (Publications, Films and Computer Games) Enforcement Act 1995* (Vic). The *Classification (Publications, Films and Computer Games) Act 1995* (Cth) was recently amended to provide for, among other things, integration of the Office of Film and Literature Classification into the Attorney-General's Department: *Classification (Publications, Films and Computer Games) Amendment Act 2007* (Cth).

79 Government of Victoria, *Submission PR 288*, 26 April 2007; Government of South Australia, *Submission PR 187*, 12 February 2007.

80 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

81 See *Gene Technology (NSW) Act 2003* (NSW); *Gene Technology Act 2001* (Vic).

82 The *Intergovernmental Agreement on Gene Technology* is discussed further below.

private sector. Organisations should be required to comply with only a single set of privacy principles.

3.54 The ALRC proposed, therefore, that the *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by the private sector. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations: *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); and the *Health Records (Privacy and Access) Act 1997* (ACT).[83]

3.55 The ALRC noted that other state and territory laws may be introduced that seek to regulate the handling of personal information in the private sector. The ALRC therefore proposed that regulations made under the *Privacy Act* should be used to exclude future state and territory laws that purport to regulate the handling of personal information by organisations.[84]

3.56 The ALRC also proposed that states and territories with information privacy legislation that purports to apply to organisations should amend that legislation so that it is no longer expressed to apply to organisations.[85]

Submissions and consultations

3.57 A large number of submissions supported the ALRC's proposals.[86] Privacy NSW, for example, supported the proposals, acknowledging that it would mean the repeal of the *Health Records Information Privacy Act 2002* (NSW) and the amendment of the *Privacy and Personal Information Protection Act 1998* (NSW) to regulate dealings with health information by NSW government agencies.[87]

3.58 The Queensland Government stated that the proposals would ensure that the rights of individuals are not dependent on the jurisdiction in which they live, and

---

83 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–1(a)–(c).

84 Ibid, Proposal 4–1(d).

85 Ibid, Proposal 4–1.

86 See, eg, Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Investment and Financial Services Association, *Submission PR 538*, 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; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Confidential, *Submission PR 519*, 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; Privacy NSW, *Submission PR 468*, 14 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.

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

would prevent organisations from 'jurisdiction shopping' to take advantage of the least onerous privacy obligations.[88]

3.59 The Cancer Council of Australia and the Clinical Oncological Society of Australia strongly supported the proposals, noting that inconsistent privacy laws impede evidence-based epidemiological health research and create cross-border barriers to monitoring of familial cancer risks.[89]

3.60 The National Health and Medical Research Council (NHMRC) strongly supported the ALRC's proposals for national legislation, but stated that unless the proposals were enacted with other structural reforms proposed by the ALRC, the complexity in the regulation of the healthcare and health and medical research sectors would not be ameliorated. It argued that it is essential that state public sectors adopt privacy regulatory regimes that deliver consistent compliance obligations across the public and private sectors. This would address the confusion and inconsistencies which impact on information exchange between the public and private sectors.[90]

3.61 The Public Interest Advocacy Centre (PIAC) supported the proposals but not the removal of state-based private sector privacy legislation, if this results in a lowering of standards of privacy protection.[91]

3.62 The Health Services Commissioner Victoria and the OVPC opposed the proposals, stating that the exclusion of the three state and territory health privacy Acts would not be necessary if federal, state and territory legislation contained uniform privacy principles and key definitions.[92]

3.63 The OVPC was concerned that, under the ALRC proposals, entirely state-owned corporations could be subject to federal jurisdiction. It also submitted that there should be a statutory obligation to consult with relevant states and territories before regulations are made to exclude laws that regulate the handling of personal information by organisations. The OVPC also argued that state contracted service providers should continue to be subject to state jurisdiction.[93]

---

88 Queensland Government, *Submission PR 490*, 19 December 2007.

89 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007.

90 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007. See also Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

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

92 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

93 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

3.64 Some stakeholders continued to argue for a single national law that would cover the state and territory public sectors, as well as the private sector and the Australian Government public sector.[94] For example, the Law Council of Australia suggested that the ALRC's proposed regime was unnecessarily complicated:

> If the Commonwealth has the necessary Constitutional power (and to the extent it does not, the States could refer such power to the Commonwealth) does the case for a complementary law regime with multiple regulators outweigh the benefit of a single, national unified privacy regime with a single, national regulator?[95]

ALRC's view

3.65 The problems associated with overlapping and inconsistent federal, state and territory laws that regulate the handling of personal information are documented throughout this Report. These problems include unjustified compliance burden and cost, impediments to information sharing and national initiatives and confusion about who to approach to make a privacy complaint.

3.66 The most appropriate way to respond to these problems is through:

- the enactment of federal legislation to regulate the handling of personal information, to the exclusion of state and territory privacy laws operating in the private sector; and

- an intergovernmental agreement that establishes an intergovernmental cooperative scheme. The scheme would provide that the states and territories should enact legislation to regulate the handling of personal information in the state and territory public sectors, applying key uniform elements such as a set of uniform privacy principles, any relevant regulations that modify the application of the principles, and relevant definitions.

3.67 Although there are a number of advantages to having a single, national privacy law administered by a single regulator, the ALRC sees merit in the arguments put forward by state governments and others that the states and territories should be left to regulate the handling of personal information in their public sectors. In particular, the ALRC notes concerns relating to the need for state and territory privacy legislation to respond to local conditions, and to interact with existing state and territory information laws such as freedom of information and public records legislation. Further, the ALRC acknowledges the advantages of having state and territory privacy regulators deal with complaints, provide advice, and perform educational functions.[96]

---

94 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007. Microsoft Asia Pacific stated, however, that if a single national law is not possible for constitutional reasons or otherwise, then there is merit in a Commonwealth-state cooperative scheme: Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

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

96 This issue is discussed in Ch 14.

3.68 While a single national privacy law could accommodate many of these concerns, the ALRC's view is that, for the time being,[97] the Australian Parliament should exercise its legislative power only in relation to the handling of personal information by the private sector and the Australian Government public sector. The ALRC recommends below an intergovernmental cooperative scheme in relation to state and territory public sectors.

3.69 Many stakeholders focused on inconsistency in the regulation of personal information in the private sector. In particular, it was suggested in submissions that various problems arise because the handling of health information in the private sector is regulated by the *Privacy Act* and state and territory legislation in NSW, Victoria and the ACT.

3.70 These issues would be dealt with effectively if organisations were required to comply with a single set of principles, and any relevant regulations that modify the application of those principles, in relation to the handling of health information. This view is consistent with the Report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), where the ALRC and the Australian Health Ethics Committee recommended that:

> As a matter of high priority, the Commonwealth, States and Territories should pursue the harmonisation of information and health privacy legislation as it relates to human genetic information. This would be achieved most effectively by developing nationally consistent rules for handling all health information.[98]

3.71 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by the private sector. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations: *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); and the *Health Records (Privacy and Access) Act 1997* (ACT).

3.72 A number of federal laws include provisions that state the Commonwealth's intention to 'cover the field'. Section 16(1) of the *Workplace Relations Act 1996* (Cth) states that the Act is intended to apply to the exclusion of a number of listed laws of a state and territory so far as they would otherwise apply in relation to an 'employee' or 'employer'.[99] The ALRC has adopted this provision as a model for its recommendation

---

97 The ALRC has recommended that the Australian Government should initiate a review in five years to consider whether national consistency has been achieved and whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors. See Rec 3–6.

98 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–1.

99 Another model is the *Corporations Act 2001* (Cth) pt 1.1A.

to exclude the operation of state and territory laws dealing with the handling of personal information by organisations.

3.73 While some stakeholders argued that state and territory laws—that apply key elements of the *Privacy Act*—should continue to regulate the handling of health information in the private sector, many private sector organisations that handle personal information and health information operate across more than one jurisdiction. These organisations should be subject to a single set of privacy principles. Greater national consistency will be achieved if the *Privacy Act* alone regulates the handling of health information in the private sector.

3.74 Other state and territory laws may be introduced that seek to regulate the handling of personal information in the private sector.[100] The *Privacy Act* should operate to exclude the operation of such laws. The ALRC has therefore recommended that regulations made under the *Privacy Act* should operate to exclude future state and territory laws that purport to regulate the handling of personal information by organisations.

3.75 States and territories with information privacy legislation that purports to apply to organisations should amend that legislation so that it is no longer expressed to apply to organisations.

3.76 The ALRC notes the observation made by the NHMRC that the complexity in the regulation of health information will not be ameliorated unless this recommendation is implemented with other structural reforms proposed by the ALRC. This is particularly the case in relation to the movement of information between the private and the public health sectors. The recommendations in this chapter are part of a package of reforms. They will need to be implemented in total if national consistency is to be achieved.

Recommendation 3–1 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

(a) *Health Records and Information Privacy Act 2002* (NSW);

(b) *Health Records Act 2001* (Vic);

100 For example, the Information Privacy Bill 2007 (WA) proposes to regulate the handling of health information by the private sector in Western Australia. Further, the *Information Privacy Act 2000* (Vic) could potentially regulate the handling of personal information by private sector organisations that are declared to be 'organisations' for the purposes of the Act: *Information Privacy Act 2000* (Vic) s 9.

(c) *Health Records (Privacy and Access) Act 1997* (ACT); and

(d) any other laws prescribed in the regulations.

Recommendation 3–2 States and territories with information privacy legislation that purports to apply to organisations should amend that legislation so that it no longer applies to organisations.

Preserving some state and territory laws

3.77 There are various state and territory laws that regulate the handling of personal information in the private sector that would need to be preserved if the Australian Government enacted national privacy legislation. For example, state and territory public health Acts require health service providers (including health service providers in the private sector) to collect and record certain information about health consumers with 'notifiable diseases', such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[101] Other state and territory laws contain provisions that require mandatory reporting for children suspected of being at risk of harm.[102] These provisions usually apply to persons who work in both the public and private sectors in areas such as health care, welfare, education, children's services, residential services, or law enforcement.

3.78 The Government of Victoria noted that there are a number of state laws that regulate the handling of personal information by both the private sector and the state public sector, for example the *Infertility Treatment Act 1995* (Vic) and the *Adoption Act 1984* (Vic).[103] The Australian Government Department of Health and Ageing also noted that a number of state laws would need to be preserved or incorporated into national legislation, such as child protection, disability and public health legislation.[104]

3.79 Stakeholders suggested a range of other state and territory laws that should be preserved under national privacy laws. These include laws mandating reporting to coroners (which may involve reporting personal information of living and deceased persons); legislation mandating reporting of ill health of health practitioners to professional registration bodies; legislative provisions that prevent disclosure of certain

101 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

102 See, eg, *Children, Youth and Families Act 2005* (Vic) pt 4.4; *Child Protection Act 1999* (Qld); *Children's Protection Act 1993* (SA) pt 4; *Children Young Persons and Their Families Act 1997* (Tas) pt 3.

103 Government of Victoria, *Submission PR 288*, 26 April 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

104 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

information relating to quality assurance activities or committees;[105] and quarantine laws that have privacy implications.[106]

3.80 In DP 72, the ALRC noted that the model UPPs would accommodate most of these laws. For example, the exception to the 'Use and Disclosure' principle in the model UPPs for use and disclosure that is 'required or authorised by or under a law' would effectively preserve many of these laws. To ensure clarity, however, the ALRC proposed that the *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'non-excluded matters' set out in the *Privacy Act*.[107]

Submissions and consultations

3.81 Some stakeholders agreed that a number of state laws that regulate the private sector would need to be preserved under national privacy legislation regulating the private sector.[108]

3.82 Other stakeholders submitted, however, that the ALRC's proposal was too complex and would cause confusion.[109] PIAC supported the proposal in principle, but expressed concern that the consultation process would be cumbersome, time consuming and likely to delay indefinitely implementation of the proposed amendments to the *Privacy Act*.

> PIAC sees no reason why the amendments can't simply be drafted in a way that lists broad categories of laws that have already been identified in submissions to the ALRC as appropriate 'non-excluded matters'. As well as laws dealing with reporting for child protection purposes and public health purposes, the list of 'non-excluded matters' should include laws regulating adoption, infertility treatment and disability service provision.[110]

---

105 See, eg, *Health Insurance Act 1973* (Cth) pt VC: National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

106 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

107 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–3.

108 See, eg, Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Tasmanian Government Department of Health and Human Services, *Submission PR 436*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

109 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

3.83 The OPC was unsure of the merits of the proposal. It submitted that the state and territory laws described in the proposal will generally fall under the various 'required by or under law' exceptions to the model UPPs; or will be authorised information handling practices and therefore meet the 'authorised by or under law' exceptions. In the OPC's view, prescribing a list of non-excluded matters may promote confusion as to the status of those state and territory laws that may otherwise satisfy an exception in the privacy principles, but which are not included on the prescribed list.[111]

ALRC's view

3.84 There are good public interest reasons why certain state and territory laws should continue to operate under national privacy legislation. For example, state and territory public health Acts require health service providers (including private sector health service providers) to collect and record certain information about health consumers with 'notifiable diseases'; and other state and territory laws contain provisions that require mandatory reporting when a child is suspected of being at risk of harm. These provisions usually apply to persons who work in both the public and private sectors.

3.85 The model UPPs would generally preserve these laws under the 'required or authorised by or under law' exception. The ALRC is concerned, however, that amending the *Privacy Act* to 'cover the field' could unintentionally exclude state and territory laws that are not preserved by any of the exceptions to the model UPPs or an exemption under the *Privacy Act*. A list of 'preserved matters'[112] will create certainty as to the state and territory laws that are preserved if the *Privacy Act* is amended to 'cover the field'.

3.86 Prescribing a list of non-excluded matters may promote confusion as to the status of those state and territory laws that may otherwise satisfy a 'required or authorised by or under law' exception in the privacy principles, but which are not included on the prescribed list. The list of 'preserved matters' should only include matters which are not covered adequately by an exception or exemption under the *Privacy Act*.[113]

3.87 The *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'preserved matters' set out in the legislation. The ALRC has adopted s 16 of the *Workplace Relations Act 1996* (Cth) as a model to deal

---

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

112 Some stakeholders advised the ALRC that they found the phrase 'non-excluded matters' confusing. The ALRC has substituted 'non-excluded matters' with the phrase 'preserved matters' to avoid any confusion.

113 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. An *exemption* applies where a specified entity or a class of entity is not required to comply with any requirements in the *Privacy Act*. The distinction between exceptions and exemptions is discussed further in Ch 33.

with state and territory laws that should be preserved under the *Privacy Act*. That section provides that the *Workplace Relations Act* operates to the exclusion of state and territory law, except in relation to a list of 'non-excluded matters'. The non-excluded matters are broad categories of laws such as 'superannuation', 'long service leave' and 'child labour'.

3.88 In DP 72, the ALRC gave a number of examples of state and territory laws that should be included in a list of 'preserved matters', including 'reporting for child protection purposes' and 'reporting for public health purposes'. While these were only examples of the kinds of matters that could be included on the list, most of them would be accommodated by the 'required or authorised by or under law' exception. The ALRC does not recommend examples of laws that should be included in the 'preserved matters' list.

3.89 If the *Privacy Act* is amended to 'cover the field', however, provisions under state and territory privacy laws that regulate the handling of personal information by organisations that contract with state and territory government agencies would be preserved. In Chapter 14, the ALRC recommends that state and territory privacy legislation should include provisions that regulate the handling of personal information by organisations when contracting with state and territory government agencies. These laws would not be covered by an exception to the model UPPs or an exemption, and should be preserved under an extended *Privacy Act*.

3.90 There are a range of other state and territory laws that regulate the handling of personal information in the private sector that should be preserved under national privacy laws. It is vital that the Australian Government consult with state and territory governments about the laws that should be preserved under an extended *Privacy Act*.

3.91 New state and territory laws may need to be preserved following the initial process of identifying 'preserved matters'. The list of preserved matters should be able to include matters prescribed in regulations to allow other matters to be added to the list from time to time.

Recommendation 3–3 The *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'preserved matters' set out in the Act. The Australian Government, in consultation with state and territory governments, should develop a list of 'preserved matters'. The list should only include matters that are not covered adequately by an exception to the model Unified Privacy Principles or an exemption under the *Privacy Act*.

An intergovernmental agreement

A cooperative scheme: Discussion Paper proposals

3.92 In DP 72, the ALRC expressed the view that national consistency will be promoted if the federal, state and territory governments enter into an intergovernmental agreement in relation to the handling of personal information. The ALRC proposed that the intergovernmental agreement should establish an intergovernmental cooperative scheme. The scheme would provide that the states and territories should enact legislation that regulates the handling of personal information in the state and territory public sectors.[114]

3.93 The ALRC noted that a number of stakeholders supported the establishment of a cooperative scheme.[115] For example, the OPC submitted that ensuring that privacy protections in state and territory jurisdictions are consistent with, and at least equivalent to, the *Privacy Act* would help to ensure national consistency. It stated that a cooperative scheme was the best way to introduce uniform privacy principles across federal, state and territory public sectors.[116]

3.94 A major cause of inconsistency in Australian privacy laws is that the *Privacy Act* and state and territory privacy laws include similar, but not identical, privacy principles. The ALRC expressed the view that the most effective method of dealing with these inconsistencies was the adoption of identical privacy principles at the federal, and state and territory level. Noting the success of complementary applied law schemes in achieving national consistency, the ALRC proposed that state and territory legislation should apply the UPPs and the *Privacy (Health Information) Regulations* as in force under the *Privacy Act* from time to time.[117]

3.95 The ALRC also proposed that state and territory privacy legislation should apply other key elements of the *Privacy Act*. The ALRC proposed that state and territory privacy laws include, at a minimum:

- relevant definitions used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information');

---

114 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–4(a).

115 See, eg, Australian Commission on Safety and Quality in Health Care, *Submission PR 252*, 14 March 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; Australian Retailers Association, *Submission PR 131*, 18 January 2007.

116 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also National Children's and Youth Law Centre, *Submission PR 166*, 1 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

117 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–4.

- provisions allowing public interest determinations (PIDs) and temporary public interest determinations (temporary PIDs);
- provisions relating to state and territory incorporated bodies (including statutory corporations);
- provisions relating to state and territory government contracts; and
- provisions relating to data breach notification.[118]

3.96 In addition, the ALRC proposed that this legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in a state or territory's public sector.[119] This aspect of the proposal is dealt with separately below.

Submissions and consultations

3.97 Many stakeholders were supportive of the ALRC's proposal for a cooperative scheme.[120] The Australian Taxation Office noted that the proposal would reduce confusion, and increase continuity and confidence for the community.[121] PIAC supported the proposal, in particular the coverage of state-owned corporations and state government contractors, and the retention of state and territory privacy regulators.[122] The School of Public Health at the University of Sydney was particularly supportive of the adoption of relevant definitions used in the *Privacy Act*.[123]

3.98 Some state bodies with responsibility for the regulation of privacy in state public sectors also supported the proposal. For example, the Health Services Commissioner Victoria supported an 'applied law' model for achieving national consistency in the privacy principles.[124] The OVPC noted that the proposal would

---

118 Ibid, Proposal 4–4(b)(i)–(v).

119 Ibid, Proposal 4–4.

120 See, eg, 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; Medicare Australia, *Submission PR 534,* 21 December 2007; Optus, *Submission PR 532,* 21 December 2007; Confidential, *Submission PR 519,* 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509,* 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; 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. The Australian Privacy Foundation stated that it would like to see more detailed options: Australian Privacy Foundation, *Submission PR 553,* 2 January 2008.

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

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

123 School of Public Health—University of Sydney, *Submission PR 504,* 20 December 2007.

124 Office of the Health Services Commissioner (Victoria), *Submission PR 518,* 21 December 2007. The Health Services Commissioner Victoria did not, however, support the amendment of the *Privacy Act* to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information: see Rec 3–1. See also Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

result in increased powers and jurisdiction for the OVPC, particularly in relation to PIDs and data breach notification.[125]

3.99 The Government of South Australia noted that, in South Australia, information privacy is regulated by an administrative instruction, not legislation. It submitted that some of the benefits of privacy legislation include the establishment of direct penalties; improved consistency between regimes; the establishment of an independent regulator with powers of investigation; improved fairness across sectoral boundaries for the management of complaints and appeals; and widening the scope of application to include local government and universities. It noted that the ALRC has not considered the benefits of an administrative instruction as opposed to a legislated instrument—in particular, the limits on the flexibility of legislation and resourcing for the management of complaints and appeals.[126]

3.100 The OPC supported the ALRC's proposal, but noted that its preferred model of health privacy law reform is to incorporate a discrete number of specific provisions in the privacy principles themselves, rather than to create a separate regulatory instrument.[127] The OPC also submitted that, while the adoption of the UPPs and the same definitions is fundamental to consistency, the other elements in the proposal, while desirable, are not crucial to consistency. The OPC was concerned that achieving agreement on those elements could hold up agreement on the UPPs and definitions. The OPC also noted that the cooperative scheme procedures may, in practice, introduce complexities that may work against achieving national consistency.[128]

3.101 The NHMRC was concerned that, if the scheme is implemented, it will be difficult to ensure consistent and sustained compliance by all states and territories. The NHMRC also noted that most public health services in Australia are operated by state and territory governments directly, but in Victoria almost all public health services are incorporated state-owned bodies with independent boards of governance. The NHMRC submitted that it will be essential to ensure that state and territory legislation applies uniformly to public health services in all jurisdictions, regardless of their legal structure.

3.102 The NHMRC also noted that the issuing of PIDs and temporary PIDs by individual jurisdictions may result in different compliance obligations which may, over time, impact on the consistency of the regulatory regime nationally. The NHMRC strongly prefers a regulatory regime which provides for the uniform adoption in all jurisdictions of PIDs and temporary PIDs that impact on the health care and health and

---

125 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
126 Government of South Australia, *Submission PR 565*, 29 January 2008.
127 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also Government of South Australia, *Submission PR 565*, 29 January 2008.
128 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

medical research sectors, following an appropriate process of inter-jurisdictional consultation.[129]

3.103 Other stakeholders did not agree with the ALRC's proposals for a cooperative scheme. The Australian Direct Marketing Association submitted that the best way to establish national consistency would be the development of harmonised legislation through the Council of Australian Governments (COAG) and the Standing Committee of Attorneys-General (SCAG) processes, or the use of the Commonwealth's constitutional head of power to extend the *Privacy Act* to 'cover the field'.[130]

ALRC's view

3.104 National consistency will be promoted if the federal, state and territory governments enter into an intergovernmental agreement in relation to the handling of personal information. The intergovernmental agreement should establish an intergovernmental cooperative scheme that provides that the states and territories should enact legislation that regulates the handling of personal information in the state and territory public sectors.

3.105 The most effective method of dealing with inconsistencies between privacy principles at the federal, state and territory level is to apply key elements of the *Privacy Act* across the jurisdictions. These elements are:

- the model UPPs and any regulations that modify the application of the UPPs (for example, the *Privacy (Health Information) Regulations*) as in force under the *Privacy Act*; and

- relevant definitions used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information').

3.106 It is important to note that not all the UPPs should be applied in state and territory legislation regulating the handling of personal information in state and territory public sectors. Some of the UPPs will not be relevant to state and territory public sectors, for example UPPs—such as UPP 6 (the 'Direct Marketing' principle)—that only apply to organisations. Further, rules relating to access and correction of personal information will need to interact with state and territory freedom of information and archives legislation. Other principles will require minor modifications to make them relevant in the context of state and territory public sectors.

3.107 The various problems caused by the use of inconsistent terms and definitions across federal information laws are outlined in Chapter 17. As noted in Chapter 17, definitions of key terms used in state and territory privacy laws generally conform to

---

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

130 Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007. See also Law Society of New South Wales, *Submission PR 443,* 10 December 2007.

those used under the *Privacy Act*. There are however some differences. Relevant definitions of key terms used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information') should be applied in state and territory laws that regulate the handling of personal information in the public sector.[131]

3.108 To promote and maintain uniformity, the ALRC recommends that the Standing Committee of Attorneys-General should adopt an intergovernmental agreement which provides that any proposed changes to key elements must be approved by an intergovernmental ministerial council.[132]

3.109 State and territory privacy laws should also include, at a minimum, a number of other important elements of the *Privacy Act*. While these provisions should be as consistent as possible to promote national consistency, absolute uniformity is not essential. The provisions are those:

- allowing PIDs and temporary PIDs;
- regulating state and territory incorporated bodies (including statutory corporations);
- regulating state and territory government contracts;
- regulating data breach notification; and
- regulating decision making by individuals under the age of 18.

3.110 To promote consistency, the ALRC has suggested below that the intergovernmental agreement could provide for a procedure that requires the states and territories to consult before amending these provisions in their own privacy legislation.

3.111 Each of these provisions is the subject of recommendations in another chapter of this Report. For example, Chapter 14 examines how inconsistency in federal, state and territory privacy law acts as an impediment to appropriate information sharing across state borders. Rather than preventing appropriate information sharing, privacy laws and regulators should encourage public sector agencies and private sector organisations to design information sharing schemes that comply with privacy laws. An effective way to facilitate information sharing between Australian Government agencies, state and territory agencies and the private sector is the adoption of the *Privacy Act* provisions that allow PIDs and temporary PIDs in state and territory laws regulating the public sectors.

---

131 Definitions of these terms are discussed in Chs 6, 62.
132 Rec 3–5.

3.112 Inconsistencies between the *Privacy Act* and state and territory privacy laws have resulted in regulatory gaps in relation to state and territory incorporated bodies (including statutory corporations) in some jurisdictions.[133] It is essential to ensure that state and territory legislation applies uniformly to public health services in all jurisdictions, regardless of their legal structure. State and territory laws that regulate the handling of personal information in the state and territory public sectors should, therefore, include provisions relating to state and territory incorporated bodies (including statutory corporations).

3.113 In Chapter 14, the ALRC notes that some state and territory privacy regimes require organisations that provide contracted services to a state or territory government agency to be bound by the relevant state or territory privacy principles for the purposes of the contract. Other state regimes provide that compliance with the state privacy regime is subject to any outsourcing arrangements, or are silent on this issue. A number of concerns were raised by stakeholders that organisations that contracted with state governments, in particular, small businesses, remain unregulated by privacy legislation. The ALRC therefore recommends that state and territory legislation regulating the handling of personal information in a state or territory's public sector should include provisions relating to state and territory government contracts.

3.114 In Chapter 51, the ALRC recommends the adoption of a data breach notification requirement. An agency (including a state or territory agency) should be required to notify the relevant regulator and any affected individual when a data breach poses a real risk of serious harm to any affected individual.[134] The ALRC notes the various benefits of this requirement, and the problems caused by an inconsistent approach to this requirement in the United States.[135] In the ALRC's view, a data breach notification requirement, based on the requirement under the *Privacy Act*, should be included in all state and territory legislation that regulates the handling of personal information.

3.115 In Chapter 68, the ALRC recommends that the *Privacy Act* be amended to make provision for determining who can make a decision on behalf of an individual under the age of 18.[136] The recommendation requires an assessment of capacity to be made, and where it is not practicable to make an assessment, apply a presumption that an individual aged 15 or over has capacity. Where an individual under the age of 18 is assessed or presumed as having capacity, he or she may make decisions under the *Privacy Act*.

3.116 The determination of capacity differs across jurisdictions and between legislative schemes. Provisions relating to determining decision-making capacity in relation to decisions regarding personal information should be the same when an individual is dealing with an organisation, or a federal, state or territory agency. State

133 See Ch 17.
134 Rec 51–1.
135 See discussion in Ch 51.
136 Rec 68–1.

and territory privacy laws should include provisions regulating decision making by individuals under the age of 18, based on the recommended provisions in the *Privacy Act*.[137]

3.117 There are advantages in having a number of agencies and bodies with responsibility for information privacy. In Chapter 17, the ALRC recommends that state and territory privacy legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in a state or territory's public sector.

3.118 The ALRC has recommended in Chapter 17 that the OPC and state and territory privacy regulators and agencies with responsibility for privacy regulation should develop and publish memoranda of understanding.[138] The issuing of PIDs and temporary PIDs by individual jurisdictions may impact on the national consistency of the regulatory regime. These memoranda of understanding should set out a process for consultation between the relevant privacy regulators and agencies when issuing PIDs and temporary PIDs, and in other circumstances such as when issuing codes and when developing and publishing joint guidance.

Recommendation 3–4 The Australian Government and state and territory governments, should develop and adopt an intergovernmental agreement in relation to the handling of personal information. This agreement should establish an intergovernmental cooperative scheme that provides that the states and territories should enact legislation regulating the handling of personal information in the state and territory public sectors that:

(a) applies the model Unified Privacy Principles (UPPs), any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act* as in force from time to time; and

(b) contains provisions that are consistent with the *Privacy Act*, including at a minimum provisions:

(i) allowing Public Interest Determinations and Temporary Public Interest Determinations;

(ii) regulating state and territory incorporated bodies (including statutory corporations);

137 Recs 68–1, 68–2, 68–3.
138 See Rec 17–3.

(iii) regulating state and territory government contracts;

(iv) regulating data breach notification; and

(v) regulating decision making by individuals under the age of 18.

A ministerial council

3.119 The OPC Review suggested that, if national consistency is to be achieved, there needs to be greater cooperation between the Australian and state and territory governments in developing legislation that has privacy implications.[139]

3.120 One option for consideration is the establishment of a permanent standing body to ensure national consistency in the regulation of personal information. Such a proposal raises a number of issues including: the membership of such a body, its functions and powers, reporting requirements, ministerial responsibility, and resourcing.

3.121 In DP 72, the ALRC considered a number of options for reform, including broadening the membership and functions of the Privacy Advisory Committee established under the *Privacy Act*.[140] The ALRC also considered a ministerial council to perform such a function. A ministerial council is generally made up of relevant ministers from the Australian Government and the states and territories who meet to discuss matters of mutual interest.

3.122 COAG is the peak intergovernmental forum in Australia. COAG comprises the Prime Minister, state premiers, territory chief ministers and the President of the Australian Local Government Association (ALGA). The COAG Secretariat is located within the Department of the Prime Minister and Cabinet. The role of COAG is to initiate, develop and monitor the implementation of policy reforms that are of national significance and which require cooperative action by Australian governments.

3.123 SCAG is a national ministerial council. Its members are the Australian Attorney-General and Minister for Justice and Customs, the state and territory attorneys-general and the New Zealand Attorney-General. Norfolk Island has observer status at SCAG meetings. SCAG seeks to achieve uniform or harmonised action within the portfolio responsibilities of its members. The types of issues that SCAG considers can be quite varied. An item is likely to be appropriate for SCAG if it:

- requires joint action from the Australian, state and territory governments;

---

139 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 43.

140 The Privacy Advisory Committee is discussed in Ch 46.

- involves the development of model or uniform model legislation; or
- is of relevance to attorneys-general.[141]

3.124 SCAG has considered privacy issues related to residential tenancy databases,[142] and is currently working on workplace privacy.[143] SCAG also has oversight of a cooperative scheme—the National Classification Scheme for film and video and for printed material. The Intergovernmental Agreement on Censorship requires that certain changes to the National Classification Scheme must be considered and agreed to by all SCAG ministers.

3.125 Another example of a ministerial council model is the Gene Technology Ministerial Council (GTMC). The GTMC oversees the implementation of the *Gene Technology Act 2000* (Cth) and the operation of the Gene Technology Regulator. The GTMC was established by an intergovernmental agreement between the Australian Government and all state and territory governments. The intergovernmental agreement also commits state and territory governments to enact corresponding state and territory legislation.[144]

3.126 The functions conferred upon the GTMC by the intergovernmental agreement include: issuing policy principles, policy guidelines and codes of practice to govern the activities of the Regulator and the operation of the scheme; approving the appointment (and, if necessary, the dismissal) of the Regulator; and considering and, if thought appropriate, agreeing on proposed changes to the scheme.[145] The GTMC is supported by the Gene Technology Standing Committee comprised of senior Australian Government and state and territory department officials, and the Regulator is supported by the Office of the Gene Technology Regulator.

3.127 In DP 72, the ALRC proposed that, to promote and maintain uniformity, SCAG should adopt an intergovernmental agreement which provides that any proposed changes to the:

- UPPs must be approved by SCAG; and
- *Privacy (Health Information) Regulations* must be approved by SCAG, in consultation with the Australian Health Ministers' Advisory Council (AHMAC).

---

141 Australian Government Attorney-General's Department, *Standing Committee of Attorneys-General* <www.ag.gov.au> at 14 April 2008.

142 See Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

143 SCAG has recently agreed that a SCAG working group should develop a model for nationally consistent workplace privacy regulation: Standing Committee of Attorneys-General, *Communiqué*, 28 March 2008.

144 The *Intergovernmental Agreement* on *Gene Technology*, cl 9.

145 Ibid, cl 9.

3.128 The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.[146]

Submissions

3.129 Many stakeholders supported the ALRC's proposal that SCAG have the role of overseeing national consistency in the regulation of personal information.[147] Some stakeholders submitted, however, that COAG would be the most appropriate body following the new Australian Government administrative arrangements.[148] It was also noted that COAG would be an appropriate forum, given the involvement of the significant privacy stakeholder group, the ALGA.[149]

3.130 The OPC suggested that any proposed changes to the *Privacy (Health Information) Regulations* be approved by SCAG in consultation with the Australian Health Ministers' Conference, comprising the health ministers of all Australian jurisdictions, rather than AHMAC, as proposed by the ALRC. The OPC also suggested that the agreement could establish a consultative process when states and territories propose to amend their own privacy regulation.[150]

3.131 Other stakeholders did not support the proposal.[151] For example, the Queensland Government preferred a national standing committee of privacy representatives selected by constituent governments to assess and endorse proposals for future reform and amendment of the privacy principles.[152] The OVPC submitted that there is some merit in the creation of a permanent standing body comprising all jurisdictions' privacy commissioners to consider and promote national consistency, information sharing

---

146 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–6.

147 See, eg, Government of South Australia, *Submission PR 565*, 29 January 2008; Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 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; Queensland Government, *Submission PR 490*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

148 The Administrative Arrangements Order of 25 January 2008 established that s 63 of the *Privacy Act* (Legal Assistance) is to be dealt with by the Attorney-General and administered by the Attorney-General's Department. Otherwise privacy matters are dealt with by the Special Minister of State, and the *Privacy Act* is administered by the Department of the Prime Minister and Cabinet: Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

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

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

151 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.

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

between regulators, cooperative arrangements for enforcement, and enhanced legislative scrutiny of bills that may impact adversely on privacy.[153]

3.132 The Australian Privacy Foundation did not support the establishment of a permanent standing body on privacy. The Foundation submitted that such bodies have 'delayed or buried privacy issues in the past'.[154]

ALRC's view

3.133 A permanent standing body would assist in maintaining national consistency in the regulation of personal information. As noted above, national consistency will be promoted if the federal, state and territory governments enter into an intergovernmental agreement to establish a cooperative scheme in relation to the regulation of personal information. The intergovernmental agreement should provide that any proposed changes to the:

- model UPPs and relevant definitions used in the *Privacy Act* (for example 'personal information' and 'sensitive information') must be approved by SCAG; and

- new *Privacy (Health Information) Regulations* and relevant definitions (for example, 'health information' and 'health services') must be approved by SCAG, in consultation with the Australian Health Ministers' Conference.

3.134 The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

3.135 SCAG is the most appropriate body to ensure national consistency as it is an established body that has experience in considering privacy issues and in promoting consistency through cooperative schemes. The ALRC acknowledges that, while the majority of state and territory ministers with responsibility for the regulation of personal information are attorneys-general, the Australian Government minister and South Australian minister responsible for information privacy are not.[155]

3.136 The ALRC has been informed that, despite changes to the Australian Government administrative arrangements, SCAG will continue to be the body to consider information privacy issues. Under this arrangement, the Cabinet Secretary

153 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.
154 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.
155 The minister responsible for information privacy in South Australia is currently the Minister for Finance.

will brief the Attorney-General of Australia on information privacy issues that need to be considered by SCAG.[156]

3.137 Further, the South Australian minister with responsibility for information privacy is able to attend SCAG meetings. SCAG adopted procedures to accommodate this situation in its oversight of the National Classification Scheme. SCAG procedures provide that where a minister responsible for censorship is not the Attorney-General, that minister attends SCAG meetings for discussion of censorship matters.

3.138 When considering any changes to the *Privacy (Health Information) Regulations*, SCAG should consult with the Australian Health Ministers' Conference, comprising the health ministers of all Australian jurisdictions, rather than AHMAC, as proposed by the ALRC in DP 72.

3.139 The ALRC sees merit in the intergovernmental agreement establishing a consultative process where states and territories propose to amend their own privacy regulation. Such a consultative process will promote and maintain national consistency.

3.140 Consultation will not be necessary every time a state or territory amends their own privacy regulation. The recommended intergovernmental agreement, however, should require the states and territories to consult with each other before amending certain elements of their own legislation. These elements include those identified by the ALRC in Recommendation 3–4 that have some impact on national consistency.

Recommendation 3–5 To promote and maintain uniformity, the Standing Committee of Attorneys-General (SCAG) should adopt an intergovernmental agreement which provides that any proposed changes to the:

(a) model Unified Privacy Principles and relevant definitions used in the *Privacy Act* must be approved by SCAG; and

(b) new *Privacy (Health Information) Regulations* and relevant definitions must be approved by SCAG, in consultation with the Australian Health Ministers' Conference.

The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

156 Australian Government Attorney-General's Department, *Correspondence*, 12 February 2008.

An expert committee

3.141 In DP 72, the ALRC proposed that SCAG should be assisted by an expert advisory committee to:

- provide advice in relation to the amendment of the proposed UPPs and *Privacy (Health Information) Regulations*;
- address issues related to national consistency such as the scrutiny of federal, state and territory bills that may adversely impact on national consistency in the regulation of personal information; and
- address issues related to the enforcement of privacy laws, including information sharing between privacy regulators and cooperative arrangements for enforcement.

3.142 The ALRC also proposed that appointments to the expert advisory committee should ensure a balanced and broad-based range of expertise, experience and perspectives relevant to the regulation of personal information. The appointments process should involve consultation with state and territory governments, business, privacy and consumer advocates and other stakeholders.[157]

Submissions and consultations

3.143 Many stakeholders supported the ALRC's proposal for the establishment of an expert advisory committee to assist a Ministerial Council.[158] The Australian Privacy Foundation supported the proposal, subject to its concerns about SCAG.[159]

3.144 It was suggested that the expert advisory committee should include:

- representatives from federal, state and territory archival organisations, or that the committee should consult with such archival organisations;[160]
- privacy regulators from throughout Australia;[161]

---

157 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–7.

158 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 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; 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.

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

160 National Archives of Australia, *Submission PR 414*, 7 December 2007.

- consumer representatives;[162] and
- possibly some government departments.[163]

3.145 Some stakeholders questioned whether an expert committee was necessary.[164] The OPC, for example, submitted that such a committee may add to bureaucratic complexity. Instead, the Office suggested that existing bodies, such as the administering agencies for Australian, state and territory information privacy laws, would be well placed to provide advice. The OPC also was concerned that the expert committee may be seen as a substitute for consultation by SCAG with relevant stakeholders on information privacy issues.[165]

ALRC's view

3.146 While the ALRC agrees that the amendment of the UPPs and the *Privacy (Health Information) Regulations* only should occur after consultation with relevant stakeholders, it is not necessary to establish an expert advisory committee to assist SCAG. Such a committee is unnecessary and may add to bureaucratic complexity.

3.147 The ALRC notes that SCAG is currently advised by the SCAG Officers Committee, and that SCAG committees have previously engaged in broad-based consultation, most recently in relation to workplace privacy. On privacy issues, such a committee usefully could consult with the public and private sectors; federal, state and territory privacy regulators and other bodies with responsibility for information privacy; bodies with responsibility for records management, including archival organisations; and privacy and consumer representatives.

3.148 SCAG might also consult with the Privacy Advisory Committee established under the *Privacy Act*[166] and the Asia Pacific Privacy Authorities (APPA) forum that meets biannually and includes the federal and state and territory privacy regulators of Australia, New Zealand, Hong Kong and South Korea.

Ensuring uniform interpretation

3.149 As noted above, national consistency will be promoted if the model UPPs and other key elements of the *Privacy Act* are adopted at the federal, state and territory level. The uniformity of these elements may be reduced over time, however, by differing interpretations of these elements by courts and tribunals.

---

161 Privacy NSW, *Submission PR 468*, 14 December 2007.
162 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
163 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.
164 Government of South Australia, *Submission PR 565*, 29 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
165 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
166 The ALRC recommends that the membership of the Privacy Advisory Committee be expanded: see Ch 46.

3.150 Under the ALRC's recommendations, the Administrative Appeals Tribunal (AAT), the Federal Magistrates Court and the Federal Court of Australia will play a significant role in maintaining uniformity in the development of jurisprudence at the federal level. As noted in Part F, privacy complaints under the *Privacy Act* should generally be dealt with by the Privacy Commissioner, with a right of appeal to the AAT and the Federal Court. Applications for civil penalties will be dealt with by the Federal Magistrates Court and the Federal Court.[167]

3.151 State and territory courts and tribunals may be required to consider state and territory privacy legislation that applies the UPPs and other key elements of the *Privacy Act*. National consistency could be undermined if state and territory courts and tribunals adopt different interpretations of the UPPs and other key elements of the *Privacy Act* applied in state and territory legislation.

3.152 While courts of appeal in each state and territory can work to ensure consistency within their jurisdictions, they cannot contribute directly to national consistency because their decisions are not binding in other jurisdictions. The principle of comity, however, is intended to encourage a degree of uniformity across jurisdictions. As the High Court of Australia stated in the context of the *Corporations Law* scheme:

> uniformity of decision in the interpretation of uniform national legislation … is a sufficiently important consideration to require that an intermediate appellate court—and all the more so a single judge—should not depart from an interpretation placed on such legislation by another Australian intermediate appellate court unless convinced that that interpretation is plainly wrong.[168]

3.153 The principle of comity will ensure a certain level of national consistency in the interpretation of the UPPs and other key elements of the *Privacy Act* applied in state and territory legislation. The ALRC also notes that the High Court of Australia plays a key role in ensuring uniformity in the development of jurisprudence in Australia.

3.154 In Chapter 17, the ALRC recommends that the OPC should develop memoranda of understanding with each of the bodies with responsibility for information privacy in Australia. The memoranda of understanding should outline processes for developing and publishing joint guidance on the interpretation of the model UPPs and other applied elements of the *Privacy Act*. This should assist bodies with responsibility for information privacy, including state and territory privacy regulators, to adopt a consistent interpretation of the UPPs and other aspects of privacy regulation.

---

167 See Chs 49 and 50.

168 *Australian Securities Commission v Marlborough Gold Mines Limited* (1993) 177 CLR 485, 492.

A review

3.155 In DP 72, the ALRC proposed that the Australian Government should initiate a review in five years to consider whether the proposed 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 to cover the field in relation to information privacy in the state and territory public sectors.[169]

Submissions and consultations

3.156 A number of stakeholders supported a review.[170] The NHMRC submitted that, while a cooperative national scheme will achieve a nationally consistent outcome, the sustainability of such an arrangement will need to be demonstrated. The NHMRC anticipated that it will be very challenging to achieve and sustain full participation by all states and territories.[171]

3.157 The National Australia Bank supported an ongoing review of the privacy regime, in the context of the public and the private sectors, technological advancements and societal changes, and to ensure consistency and removal of duplication between federal, state and territory legislation.[172]

3.158 Privacy NSW supported the proposal, but affirmed its view that the *Privacy Act* should not cover the field in relation to information privacy because state and territory regulation achieves better compliance outcomes.[173]

3.159 Other stakeholders opposed the proposal. For example, the Queensland Government submitted that Commonwealth legislation covering the state and territory public sectors would impinge on the independence of the state and territory governments to regulate the handling of their own information.[174]

3.160 The OVPC also opposed the proposal. It submitted that a national privacy law could impact negatively on the enforcement and other functions associated with privacy regulation, if regulation is to be the sole province of a single national office. The OVPC also submitted that, given the complexities of the consultative process by

---

169 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–5.

170 See, eg, Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Confidential, *Submission PR 519*, 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; 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.

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

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

173 Privacy NSW, *Submission PR 468*, 14 December 2007. See also Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

174 Queensland Government, *Submission PR 490*, 19 December 2007.

which uniform legislation and regulatory structures would need to be established, ten years may be a more appropriate or practical timeframe.[175]

3.161 The Government of South Australia did not support the proposal. It also argued that five years is not enough time to allow states and territories to enact and implement legislation and necessary administrative and cultural changes.[176]

ALRC's view

3.162 The Australian Government should initiate a review in five years from the commencement of the amended *Privacy Act* to consider whether the proposed intergovernmental scheme in relation to the handling of personal information in state and territory public sectors has achieved its goal. The review should consider whether it would be more effective for the Australian Parliament to cover the field in relation to information privacy in the state and territory public sectors.

3.163 The ALRC does not recommend that the Commonwealth should legislate in relation to information privacy in the state and territory public sectors. Rather, the recommendation is that the review should consider this issue. Extending the operation of the *Privacy Act* to cover state and territory public sectors is just one option. The review could also consider whether the *Privacy Act* should be extended to cover certain elements of state and territory public sectors and not others. For example, the *Privacy Act* could be extended to apply to state and territory statutory corporations and other bodies such as public hospitals and universities. The states and territories should be consulted as part of the review.

Recommendation 3–6 The Australian Government should 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.

Other methods to achieve national consistency

3.164 This section of the chapter summarises various methods for dealing with inconsistency and fragmentation in the regulation of personal information. Some of these methods are discussed in detail in other chapters of this Report.

175 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
176 Government of South Australia, *Submission PR 565*, 29 January 2008.

Codes made under privacy legislation

3.165 In Chapter 48, the ALRC states that organisations and industries should retain the ability to flesh out the requirements of the privacy principles in privacy codes approved by the Privacy Commissioner under Part IIIAA of the *Privacy Act*; and that codes could be made binding under the regulation-making power recommended by the ALRC.[177]

3.166 State and territory privacy commissioners have the power to develop codes under some state and territory privacy legislation.[178] The ALRC notes the potential for inconsistency in privacy regulation to occur as a result of different privacy commissioners issuing privacy codes in different jurisdictions.

3.167 In Chapter 17, the ALRC recommends that the OPC and state and territory privacy regulators and agencies with responsibility for privacy regulation should develop and publish a memorandum of understanding. In the ALRC's view, this memorandum of understanding should set out a process for consultation with privacy commissioners in other jurisdictions when the OPC is developing codes under the *Privacy Act*, or when state and territory privacy commissioners are developing codes under state or territory privacy legislation.[179]

Joint guidance

3.168 In its submission to this Inquiry, the OPC noted that providing greater guidance on the operation of existing laws, and how they relate to other regulations, will help harmonise current privacy laws.[180] In DP 72, the ALRC made a number of proposals for the OPC and other bodies to develop and publish guidance. For example, the ALRC proposed that the OPC provide further guidance on the model UPPs. The OVPC responded to these proposals noting that such guidance should be prepared jointly or in consultation with state and territory privacy commissioners, so that both the content of legislation and the interpretation and procedures of privacy commissioners can be as consistent as possible.

3.169 In the ALRC's view, a memorandum of understanding between the OPC and state and territory privacy regulators could outline a consultation process when developing guidance on the UPPs and the *Privacy (Health Information) Regulations*. In Chapter 17, the ALRC recommends that the OPC and state and territory privacy regulators and agencies with responsibility for privacy regulation should develop and publish a memorandum of understanding that includes a process for the development and publication of joint guidance.

---

177 See Chs 4, 48.
178 See Ch 2.
179 See Rec 4–6.
180 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

Rules and guidelines

3.170 The potential for inconsistency and complexity to arise because of the development of privacy rules and guidelines by agencies and organisations is discussed in Chapter 17. Organisations and agencies should consult with the OPC when developing privacy rules and guidelines.

Privacy impact statements

3.171 In DP 72, the ALRC considered whether a 'privacy impact statement' should accompany any federal, state and territory government proposal to introduce legislation that impinges on privacy.[181] Such a statement could include a privacy impact assessment and an analysis of whether the government proposal is consistent with existing federal, state and territory laws relating to the regulation of privacy. This may include consideration of privacy matters other than the protection of personal information.

3.172 The ALRC has not recommended that a privacy impact statement should accompany every federal, state and territory government proposal to introduce legislation that impinges on privacy. A mandatory requirement of this kind would involve an unjustified compliance burden and cost.

3.173 The ALRC has recommended, however, that the *Privacy Act* should be amended to empower the Privacy Commissioner to direct an agency to provide to the Privacy Commissioner a Privacy Impact Assessment (PIA) in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[182]

3.174 New government projects will often require the enactment of legislation. When a government agency is conducting a PIA of a new project that is supported by legislation, the assessment should address how the new legislation will interact with existing federal, state and territory privacy laws. This should help to maintain national consistency. PIAs are considered in detail in Chapter 47.

---

181 N Waters, *Consultation PC 17*, Sydney, 2 May 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

182 Rec 47–4.

4. Regulating Privacy

Contents

Introduction

4.1 This chapter sets out the ALRC's approach to regulating privacy at the federal level in Australia.[1] In summary, the ALRC's approach draws heavily on the theory of principles-based regulation, with privacy principles being the primary method of regulation used in the *Privacy Act 1988* (Cth). These principles are not adequate, however, to achieve the relevant policy objectives in all the areas covered by the *Privacy Act*. In such areas, the ALRC recommends more prescriptive or different rules, through the use of regulations or other legislative instruments, in order to achieve such objectives.

4.2 The chapter is divided into three sections. The first examines the theory of principles-based regulation and compliance-oriented regulation, which are the twin

1 The model for achieving consistency in privacy regulation across Australia is examined in Ch 3.

foundations of the approach adopted by the ALRC in this Report. The second section sets out the ALRC's approach to regulating privacy, both in terms of the regulatory tools and the approach to regulation. This section applies the theory discussed in the first section and outlines the areas where, and the reasons why, the ALRC has moved away from pure principles-based regulation. The third section sets out the scope for co-regulation in the ALRC's approach.

4.3 This chapter does not set out recommendations for reform. The purpose of the chapter is to outline the approach adopted by the ALRC for regulating privacy in Australia, which in turn informs the discussion in this Report.

Regulatory theory

4.4 Principles-based regulation is the primary method that should be used to regulate information privacy in Australia.[2] By principles-based regulation, the ALRC is referring to both the tools of regulation—that is, the principles—and adopting a more outcomes-based approach to regulating privacy.[3] This section will examine in turn the theory of principles-based regulation and the notion of an outcomes-based—or 'compliance-oriented'—approach to regulation.

Principles-based regulation

4.5 Principles-based legislation relies on principles to articulate the outcomes to be achieved by the regulated entities. According to Professor Julia Black, principles are 'general rules … [that] are implicitly higher in the implicit or explicit hierarchy of norms than more detailed rules: they express the fundamental obligations that all should observe.' Black states that principles-based regulation avoids 'reliance on detailed, prescriptive rules and rel[ies] more on high-level, broadly stated rules or principles'.[4]

4.6 Part of the guiding purpose of a principles-based approach is to shift the regulatory focus from *process* to *outcomes*. The rationale for this is described as follows:

> Regulators, instead of focussing on prescribing the processes or actions that firms must take, should step back and define the outcomes that they require firms to achieve. Firms and their management will then be free to find the most efficient way of achieving the outcome required.[5]

---

2 The development of privacy principles and the recommended form of the Unified Privacy Principles is discussed in more detail in Ch 18.

3 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 3.

4 Ibid, 3. Ch 18 provides examples of the three regulatory methods of principles, bright line rules and complex/detailed rules.

5 Ibid, 5.

4.7 Principles-based regulation can be distinguished from rules-based regulation in that it does not necessarily prescribe detailed steps that must be complied with, but rather sets an overall objective that must be achieved. In this way, principles-based regulation seeks to provide an overarching framework that guides and assists regulated entities to develop an appreciation of the core goals of the regulatory scheme. A key advantage of principles-based regulation is its facilitation of regulatory flexibility through the statement of general principles that can be applied to new and changing situations. It has been said that such a regulatory framework is exhortatory in that it emphasises a 'do the right thing' approach and promotes compliance with the spirit of the law.[6]

4.8 According to Black, all forms of regulation are subject, to varying degrees, to the following problems:

- *Rules are just a 'best guess' as to the future*: The rule maker has to anticipate how the rule will be applied in the future. New situations may arise that were not expected/known about when the rule was written, and the rule may be interpreted and applied in ways that were not intended or anticipated by the writer.
- *Rules are never perfectly congruent with their purpose …* : Rules are inevitably either under-inclusive, failing to catch things that the rule maker might want to catch, and/or over-inclusive, catching things that the rule maker might not want to catch when applied to particular sets of circumstances …
- *Whether a rule is clear or certain depends on shared understandings*: Just looking at a rule does not tell us whether it is certain. … Whether or not a rule is 'certain' depends not so much on whether it is detailed or general, but whether all those applying the rule (regulator, regulated firm, court/tribunal) agree on what the rule means.
- *How a rule affects behaviour does not depend solely on the rule*: … whether a rule has the desired effect on behaviour depends only partly on whether it is a precise, detailed rule or whether it is a principle. The firm's own attitude to regulation, the incentive structures for compliance and non-compliance, and the approach taken to enforcement, are also critical.[7]

4.9 Principles-based regulation attempts to solve these problems, largely by providing greater 'flexibility', thereby allowing for 'a greater degree of "future-proofing", enabling the regime to respond to new issues as they arise without having to create new rules'.[8] Future-proofing can be achieved by drafting purposive principles that both express the rationale for the rule and provide 'overarching requirements that

6 S Arjoon, 'Striking a Balance Between Rules and Principles-Based Approaches for Effective Governance: A Risks-Based Approach' (2006) 68 *Journal of Business Ethics* 53, 58.

7 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 8.

8 Ibid, 7.

can be applied flexibly to a rapidly changing industry'. Principles-based regulation also makes use of qualitative and often evaluative terms such as fair, reasonable and suitable.[9] This regulatory approach can facilitate compliance as it allows entities to honour the spirit of the law by developing policies or other mechanisms that simultaneously comply with the rule and meet the entity's needs.

4.10 By contrast, rules-based regulation is comparatively rigid. Detailed rules impose requirements that are not always appropriate for all entities regulated by the relevant scheme and, further, they do not always cover all of the entities or activities that are intended to be regulated.[10] Black states:

> Detailed rules, it is often claimed, provide certainty, a clear standard of behaviour and are easier to apply consistently and without retrospectivity. However, they can lead to gaps, inconsistencies, rigidity and are prone to 'creative compliance', to the need for constant adjustment to new situations and to the ratchet syndrome, as more rules are created to address new problems or close new gaps, creating more gaps and so on.[11]

4.11 On the other hand, a regulatory approach that is based on using prescriptive rules can provide greater clarity in the regulation, as it is easier for a regulated entity to determine what rules it must comply with and the minimum standards of compliance expected.[12] This, in turn, can direct responsibility for the regulatory system away from the entities being regulated.[13]

4.12 Proponents of principles-based regulation argue that, contrary to the assertions of clarity and certainty, rules-based regulation 'can be a dead hand on technology and product innovation'.[14] For example, the former Parliamentary Secretary to the Treasurer, the Hon Chris Pearce MP, has argued that rules-based regulation introduces 'unnecessary legal complexity' and encourages 'box-ticking' exercises, rather than complying with the spirit and intent of the law.[15]

4.13 The disadvantages of a principles-based system centre on problems of ambiguity, which can undermine the system's intended protections and accountability:

> Principles are criticised for not providing certainty; for creating an unpredictable regulatory regime in which regulators can act retrospectively; for allowing firms to

---

9 Ibid, 4.

10 O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 330–331.

11 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 7.

12 See O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 331.

13 Investment and Financial Services Association, *Towards Better Regulation: Policy on Future Regulation of Financial Services in Australia* (2006), 3.

14 Ibid, 3, rec 1.

15 C Pearce, 'The Future of Governance Regulation in Australia' (Paper presented at 21st National Conference of Chartered Secretaries Australia, 22 November 2004).

> 'backslide', and get away with the minimum level of conduct possible; and thus for providing inadequate protection to consumers or others.[16]

4.14 Principles-based regulation often deals with this lack of clarity and certainty by integrating principles with other forms of regulation. For instance, detailed rules can be used to supplement principles; official guidance can be issued to explain the principles; and dialogue can be facilitated between the regulator and regulated entities.[17]

4.15 Further, depending on the features of the regulatory scheme, principles-based regulation may also provide greater clarity through the interpretation of the principles by a regulatory body and the enforcement of those interpretations across the regulated industry or group.[18] This leads to the development of a body of precedent that clarifies the principles and provides entities with further guidance.

4.16 The emphasis on outcomes in principles-based regulation allows regulated entities to work towards the effective implementation of the principles within their own organisational context without dwelling on the 'expensive legislative focus'.[19] Thus, in the privacy law context, the Privacy Commissioner, Karen Curtis, stated:

> By encouraging organisations to recognise the business advantages of good personal information handling practices and regulating their behaviour accordingly, government regulators can minimise regulatory intervention and red tape. This has been a common theme of our regulatory approach where a legislative framework is balanced by an emphasis on business privacy awareness and self-regulation. The idea is to inculcate the values and objectives of privacy law in business rather than just the superficial rules. When this happens organisations will be better equipped to deal with technological change because they will understand the ideas behind the laws—the principles—and will not become as confused by detailed technology-specific regulations.[20]

4.17 In this way, principles-based regulation aims to minimise the need for enforcement by 'encouraging organisations to understand the values behind the law and change their behaviour accordingly; not because they might get caught out by a regulator, but because they understand why the law is there and what its objectives are'.[21] This has been described as 'nurturing a culture of voluntary compliance with the

---

16 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 2.

17 Ibid, 15.

18 An example is the United Kingdom's Financial Services Authority, as discussed in Ibid, 15 .

19 S Arjoon, 'Striking a Balance Between Rules and Principles-Based Approaches for Effective Governance: A Risks-Based Approach' (2006) 68 *Journal of Business Ethics* 53, 55.

20 K Curtis, 'Reducing Overlap, Duplication and Inconsistency' (Paper presented at Australian Regulatory Reform Evolution 2006, Canberra, 24 October 2006), 17.

21 Ibid, 13.

law'.[22] Nevertheless, Black and others emphasise that breach of a principle should involve an element of fault and public sanction.[23]

4.18 Although rules-based and principles-based regulation are very different in their approach, in many instances they can operate as a hybrid system, providing regulated entities with the benefits of both systems. In many established systems of regulation, high-level principles that can be applied flexibly to new situations and promote a best practice approach to regulation are complemented by detailed rules providing clarity.

Compliance-oriented regulation

4.19 As noted above, the concept of principles-based regulation embraces both the tools of regulation and the approach to administering those tools.[24] Compliance-oriented regulation adopts 'an outcomes-based approach to total regulatory design',[25] in which 'all the factors of regulatory rule making, monitoring, and enforcement are designed to elicit a particular regulatory objective'.[26]

4.20 Dr Christine Parker has identified a number of elements of compliance-oriented regulation, which the ALRC has grouped for convenience into: securing voluntary compliance with the regulatory objectives; undertaking informed monitoring for non-compliance; and engaging in enforcement actions where voluntary compliance fails.[27]

4.21 Parker explains that the first step of compliance-oriented regulation is 'providing incentives and encouragement to voluntary compliance and nurturing the ability for private actors to secure compliance through self-regulation, internal management systems, and market mechanisms where possible'.[28] A key way a regulator can help foster an agency's or organisation's capacity to comply is through education, guidance and other assistance.[29]

4.22 The second element of compliance-oriented regulation is 'informed monitoring for non-compliance'.[30] Monitoring must be used 'to determine whether regulatory design is having its desired effect on the target population'.[31] As regulators cannot

---

22 Australian Transactions Reports and Analysis Centre, *AUSTRAC Supervisory Framework* <www.austrac.gov.au/files/supervisory_framework.pdf> at 14 April 2008, 4.

23 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 4. See also Australian Transactions Reports and Analysis Centre, *AUSTRAC Supervisory Framework* <www.austrac.gov.au/files/supervisory_framework.pdf> at 14 April 2008, 4.

24 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 3.

25 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 531.

26 Ibid, 535.

27 Ibid, 535.

28 Ibid, 539.

29 Ibid, 554.

30 Ibid, 535.

31 Ibid, 537.

enforce every rule or cover every problem, they should use information collected about the regulatory problem to develop a 'risk-based approach to targeting inspections'.[32]

4.23 A compliance-oriented regulatory design also must provide for enforcement in the event of non-compliance; this is the third element. A regulator's response to non-compliance in a principles-based regime can be likened to rehabilitative, rather than punitive, justice. As Parker explains, when organisations fail to comply in the first instance, the preferred approach in compliance-oriented regulation would be to 'attempt to restore or nurture compliance rather than reverting immediately to a purely punishment-oriented approach'.[33]

4.24 It is critical, however, that these attempts to nurture and restore compliance operate in the presence of more punitive sanctions, as the evidence shows that 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.[34]

> The idea is that regulators should engage tit for tat in restorative or persuasive enforcement strategies depending on the responses of the regulated entity. A regulator can start with persuasive or restorative strategies and then move to more punitive strategies if voluntary compliance fails. If the application of punitive sanctions succeeds in bringing about compliance, then the regulator can revert to a trusting demeanour. If it does not bring about compliance, then the regulator must invoke harsher sanctions. The wider the range of strategies (from restorative to punitive) available to the regulator, the more successful tit-for-tat enforcement is likely to be.[35]

4.25 This principle is encapsulated in Professors Ian Ayres and John Braithwaite's enforcement pyramid.[36] Braithwaite contends that compliance is 'most likely' when a regulator displays an explicit enforcement pyramid:

> Most regulatory action occurs at the base of the pyramid where initially attempts are made to coax compliance by persuasion. The next phase of enforcement escalation is a warning letter; if this fails to secure compliance, civil monetary penalties are imposed; if this fails, criminal prosecution ensues; if this fails, the plant is shut down or a licence to operate is suspended; if this fails, the licence to do business is revoked.

---

32 Ibid, 537.

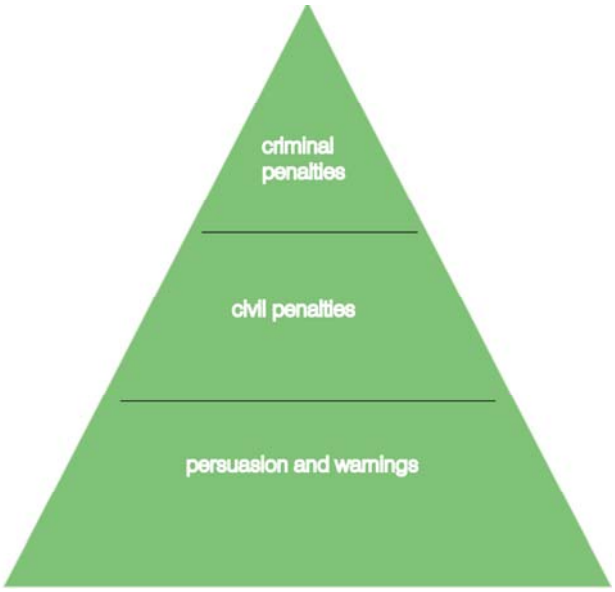
33 Ibid, 539.

34 Ibid, 541. See also J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 4.

35 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 541.

36 The model was first put forward by Braithwaite in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985). See also 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.

> The form of the enforcement pyramid is the subject of the theory, not the content of the particular pyramid.[37]



4.26 Self-regulation and co-regulation also form part of the enforcement pyramid model. It has been argued that regulatory responses should not be confined to escalations up the enforcement pyramid, but should also consider industry responses or allowing instruments to be implemented by trade associations and professions as well as regulators.

> Seeing regulation in terms of these dimensions allows creative mixes, or networks, of regulatory enforcement instruments and of influencing actors or institutions to be adopted. It also encompasses the use of control instruments that, in certain contexts, may be easier to apply, less costly and more influential than state controls.[38]

ALRC's preference for principles-based regulation

4.27 The ALRC adopts principles-based regulation as its guide in developing the tools for regulating privacy for several reasons.

4.28 First, the ALRC is of the view that principles have greater flexibility in comparison to rules. Being high-level, technology-neutral and generally non-prescriptive, principles are capable of application to all agencies and organisations

---

37 Quoted in F Haines, *Corporate Regulation: Beyond 'Punish or Persuade'* (1997), 218–219.

38 R Baldwin and J Black, *Really Responsive Regulation* (2007), LSE Law Society and Economy Working Paper 15 (2007), 11.

subject to the *Privacy Act*, and to the myriad of ways personal information is handled in Australia.

4.29 Secondly, as outlined above, principles allow for a greater degree of 'future-proofing' and enable the regime to respond to new issues as they arise without having to create new rules.[39]

4.30 Thirdly, the ALRC recognises the considerable support by stakeholders for retaining principles as the primary regulatory method in the *Privacy Act*, which is discussed in more detail in Chapter 18.

Hybrid regulatory system

4.31 While the *Privacy Act* can be described as a 'principles-based regime', it is important to recognise that the ALRC's adopted approach is not a pure form of principles-based regulation. In order to achieve the necessary policy outcomes, the ALRC adopts a pragmatic approach to its regulatory model, drawing significantly on principles-based regulation as its foundation, but allowing for a reversion to more traditional rules-based regulation where appropriate.

4.32 This pragmatic approach arises out of the recognition that despite the overall benefits of principles-based regulation, the regulatory method also has its limitations. First, this type of regulation can lack certainty: agencies and organisations subject to the Act may have trouble understanding the exact requirements of the principle, and how it should apply or comply with the principles in its day-to-day operations. The second difficulty of principles-based regulation in the privacy context is that the same principles may not be appropriate to achieve the policy objectives in all the areas covered by the *Privacy Act*. In some instances, more prescriptive or different regulation may be required.

4.33 For these reasons, the ALRC is not recommending the adoption of a pure form of principles-based regulation. Having regard to the wide remit of the *Privacy Act*, the ALRC takes a pragmatic approach in drafting the regulatory tools, adopting what could be described as a hybrid model.

4.34 The approach adopted by the ALRC is a hybrid model in two respects. First, the principles themselves are not uniformly 'principles', in the theoretical sense explained above. While some of the model Unified Privacy Principles (UPPs) recommended by the ALRC are high-level and set out objectives to achieve without much prescription, others are a hybrid between high-level principle and more prescriptive rule. For example, UPP 5 sets out relatively detailed rules related to the use and disclosure of

39 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 7.

personal information, whereas UPP 7 provides a broad, high-level principle relating to data quality.[40]

4.35 Secondly, the overall regulatory model adopted by the ALRC is a hybrid system of principles and rules. While principles-based regulation forms the foundation of the ALRC's approach, the model allows for these principles to be supplemented by more specific rules in regulations or other legislative instruments, to accommodate different industries or different policy considerations.

4.36 This Inquiry considers a number of areas that pose particularly important or difficult privacy problems, such as health, research, and credit reporting. In relation to each of these areas, the ALRC's approach is to identify the appropriate balance that should be struck between allowing agencies and organisations to find their own way to achieving the object of the principle and providing more traditional, prescriptive regulation. The ALRC's approach allows for the adoption of a more rule-based approach to regulation, either to complement or supplant the privacy principles, in order to achieve the policy objectives.

4.37 The advantage of a hybrid system is that it is a practical, pragmatic response to the competing needs of clarity, flexibility, simplicity and certainty. Such a system seeks to take the advantages of both a principles- and a rules-based system in order to achieve a regulatory regime that appropriately balances clarity, enforceability and flexibility.[41] This approach also recognises that stringent adherence to principles-based regulation would not, in some instances, achieve the necessary policy outcomes.

Forms of regulation

4.38 In the ALRC's principles-based, hybrid approach, the rules relating to privacy are located in a combination of the following:

- primary legislation;
- regulations and other legislative instruments; and
- non-binding guidance issued by the Office of the Privacy Commissioner (OPC).

4.39 These three forms of regulation are intended to operate together and complement each other. Together they make up the ALRC's recommended approach to regulating privacy in Australia. Each level of regulation is discussed in detail below.

---

40 This hybrid approach is also reflected in the Information Privacy Principles and the National Privacy Principles in the *Privacy Act*, both of which have their genesis in the Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). For further discussion of privacy principles, see Ch 18.

41 O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 332.

Primary legislation

4.40 The primary legislation regulating privacy at the federal level is the *Privacy Act*. In Chapter 5, the ALRC recommends that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity. In particular, the ALRC recommends that the *Privacy Act* should be redrafted so that it is relatively brief and uncluttered, and contains the following key elements:

- objects and purposes of the legislative regime, as recommended by the ALRC in Chapter 5;
- mechanical provisions, including definitions and regulation-making powers;
- privacy principles, which will provide the core requirements of privacy law and will apply to agencies and organisations; and
- constituent and operational provisions for the OPC, including the provisions setting out the OPC's functions and powers.

4.41 Redrafting the *Privacy Act* in this way will result in a clear, concise and user-friendly document that would be capable of being understood and applied by the agencies and organisations—large and small—that will be subject to the regime. In this way, the ALRC hopes to reduce compliance costs associated with interpreting the *Privacy Act*, and to make the transition for small businesses to privacy regulation as simple as possible.

Regulations and other legislative instruments

4.42 In the ALRC's approach, the next level of regulation after the primary legislation is subordinate legislation, being regulations and other legislative instruments. These two regulatory tools introduce the second notion of the hybrid system discussed above and enable flexibility in the regulatory scheme to address specific areas that either merit particular privacy protection or require a lessening of privacy protection to enable a freer flow of information. Certain areas within the privacy sphere require more or less detailed protection to achieve the desired policy outcome.

Regulations

4.43 Under the ALRC's recommended model, regulations can be introduced to provide greater specificity and certainty in regulating privacy in relation to particular activities. Those regulations would be more detailed and specific than the privacy principles and, where appropriate, they would be able to derogate from the requirements in the privacy principles, by providing different (that is, more or less

stringent) requirements than are provided for in the principles (while remaining consistent with the objects of the Act).

4.44 The minister responsible for administering the *Privacy Act*[42] should be responsible for introducing regulations to cover these activities, rather than the OPC. This approach better conforms with the principles of responsible government and parliamentary supremacy, by clearly vesting in Parliament the power to control the rules that apply to privacy. Secondly, this approach would not exclude the OPC from the process of formulating these regulations. Rather, there would be a requirement to consult with affected parties in this process, and this is highly likely to include the OPC, as well as any relevant stakeholders.[43]

Credit Reporting Regulations

4.45 Credit reporting provides an example of where there are strong policy reasons for further prescription in relation to the collection, use and disclosure of personal information.[44] In such circumstances, a broad principle may not be considered specific enough to achieve the desired regulatory outcome.

4.46 For example, in the credit reporting context there is a public interest in specifying exactly what types of information a credit reporting agency can collect and disclose. The model UPP 2, which provides that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities, is not considered sufficiently specific or prescriptive. Under the ALRC's approach, this principle is supplemented by the recommended *Privacy (Credit Reporting Information) Regulations*, which specify the permitted content of credit report information.[45]

Health Services Regulations

4.47 In the provision of health services and the conduct of research, there are different policy considerations at stake in relation to privacy. In particular, there is a strong public interest in allowing a freer flow of information to facilitate better health outcomes and for the prevention of harm. In such circumstances, it may be necessary to derogate from a privacy principle in order to allow for greater information sharing, within set parameters.[46]

4.48 For example, the proposed *Privacy (Health Information) Regulations* allow health service providers to disclose an individual's genetic information without consent to a genetic relative of that individual, if the provider believes that the

---

42 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

43 This is provided for in *Legislative Instruments Act 2003* (Cth) ss 17–19.

44 The regulatory framework for credit reporting is discussed in Ch 54.

45 See Ch 54.

46 The regulatory framework for health services and research is discussed in Ch 60.

disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of the genetic relative. This provision, while derogating from the usual principles in relation to disclosing sensitive information, recognises the shared or familial nature of genetic information and the public interest in sharing that information with potentially affected individuals. Any such disclosure must be done in accordance with binding rules developed by the National Health and Medical Research Council (NHMRC) and approved by the Privacy Commissioner.

Other legislative instruments

4.49 In the approach adopted by the ALRC, further prescription, guidance and flexibility can also be provided through legislative instruments issued or approved by the Privacy Commissioner.

Public Interest Determinations

4.50 Such legislative instruments include Public Interest Determinations, which waive the obligation to comply with a principle such that an act or practice that would otherwise breach a privacy principle will be taken not to be an interference with privacy.[47] Public interest determinations provide the Privacy Commissioner with the flexibility to address situations where the public interest is in conflict with the privacy principles. The history of privacy regulation at the federal level would suggest that this is a fairly rare occurrence; the Commissioner only has found it necessary to issue nine Public Interest Determinations in the *Privacy Act*'s 20 years of operation. It remains, however, a useful component of the regulatory framework and one that allows greater flexibility in the privacy regime. The ALRC also notes that Public Interest Determinations are disallowable by Parliament, and therefore are subject to Parliamentary oversight.

Part IIIAA privacy codes

4.51 Another type of legislative instrument that can be used to elaborate on the requirements of the principles is a privacy code approved under Part IIIAA. These codes are discussed in detail in Chapter 48, with the ALRC recommending that the code provisions be changed so that: a code applies in addition to the UPPs and does not replace them; and the primary purpose of a code is to prescribe how a principle is to be applied or complied with.

4.52 Privacy codes, under the current provisions and the ALRC's recommended changes, cannot derogate from the principles in the way that subordinate legislation, such as regulations, can. This is a very important distinction. For the reasons set out above, the ALRC has formed the view that only the regulations should be able to

47 Public interest determinations are discussed in detail in Ch 47.

derogate from the principles established by Parliament in the *Privacy Act*. The Privacy Commissioner, while almost certainly involved in the consultation and development process for regulations, will not have the power to promulgate regulations or codes that weaken (or strengthen) the principles; that will be Parliament's responsibility.

4.53 The ALRC's approach, however, does have the flexibility to allow codes to be incorporated in regulations, similar to Part IVB of the *Trade Practices Act 1974* (Cth). The responsible minister, in consultation with the OPC and other relevant stakeholders, could choose to adopt a code and transform it into regulation, thereby allowing greater industry involvement in the regulatory sphere. As the minister is using the recommended regulation-making power, the code could contain provisions that derogate from the privacy principles.

Rules

4.54 Another type of legislative instrument under the Act is a rule, issued or approved by the Commissioner. Currently referred to as guidelines, the ALRC has recommended that they be renamed rules to reflect their binding nature.[48]

4.55 An example of the application of rules in the *Privacy Act* is to allow the collection, use and disclosure of personal and health information for health and medical research. While most research is conducted on the basis of consent from participants, the *Privacy Act* recognises that in some circumstances it is very difficult or impossible to conduct research that may be in the public interest—for example, epidemiological studies of the distribution and determinants of disease in large populations—in a way that complies with the Act. In these circumstances, the Act provides a mechanism to allow such research to go forward, subject to rules issued by the NHMRC and approved by the Privacy Commissioner. Any such research must be approved by a Human Research Ethics Committee, which must be satisfied that the public interest in the research outweighs the public interest in maintaining the level of privacy protection provided by the Act.

Guidance

4.56 Guidance is the third part of the regulatory approach adopted by the ALRC. It should be seen as sitting at the base of the regulatory model, in the sense that it is non-binding and, unlike primary and subordinate legislation, does not set out rules or obligations.

4.57 Guidance plays a particularly significant role in a regime like the *Privacy Act*. Notwithstanding the fact that the model privacy principles may be supplemented by more specific regulation in certain areas, it is still the case that the principles will form the primary method of regulation under the Act and apply to all agencies and

48 See Rec 47–2.

organisations. For agencies and organisations that do not deal with personal information that is subject to specific regulations, such as health or credit reporting information, the model privacy principles will be the primary, and possibly only, source of privacy obligations.

4.58 While principles may appear simple to apply, problems may arise in interpreting what is required to be in compliance. Whether a principle is certain depends on whether there is general consensus about what is required to achieve compliance. For these reasons, guidance from the regulator is critical to assist regulated bodies to interpret and apply the privacy principles.

4.59 Such guidance should not be considered a luxury or an add-on to the core privacy regime; the ALRC's recommended regime cannot operate effectively unless there is such guidance. The ALRC recognises, however, the tension presented by guidance as a regulatory tool. While intended by the regulator as suggestions for compliance, it can be understood by the regulated entity as binding rules that must be applied to achieve compliance. If the regulated entity treats guidance in this way, and there is a proliferation of guidance, the administration of a principles-based regime is undermined.[49] It can also deprive the regulator of the benefits of a principles-based approach by 'creating expectations as to its own conduct in the future'. That is, while the regulator may see guidance as advisory only, some regulated entities may understand it as being the definitive interpretation of the principles.[50]

4.60 Thus guidance should be published, but care should be taken that it is published only where appropriate. It is important to recognise, however, that it is not an alternative for a regulator of a principles-based regime to refuse to publish guidance where there is a genuine need. It is neither appropriate nor effective to refuse to publish guidance to help organisations and agencies understand their obligations and instead wait for them to make a mistake and breach the law. Further, such a refusal to publish guidance is inconsistent with the regulator's focus on fostering and securing compliance with principles.

4.61 It is important to make clear in publishing guidance that an agency or organisation can be in compliance with a privacy principle but not in compliance with the Commissioner's guidance; that is, the guidance is not legally binding. Such a situation is likely to be rare, but the OPC acknowledges this prospect in its non-binding guidance. For example, the guidelines on the use of data-matching in Commonwealth administration explains that the guidelines 'aim to encourage a higher standard of regard for people's privacy rights in relation to data-matching than is required by bare

---

49 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 15–16.

50 Ibid, 16.

compliance with the IPPs and an agency would not necessarily breach the IPPs if it did not adhere to these guidelines'.[51]

ALRC's preference for compliance-oriented regulation

4.62 With its focus on achieving outcomes, compliance-oriented regulation provides a useful framework to administer a principles-based regime such as the *Privacy Act*. The theory on which compliance-oriented regulation is based provides a prism through which to view and assess the compliance model underpinning the Act and the approach taken by the OPC to fostering compliance. It also provides an holistic approach for considering which regulatory strategies would best achieve the objectives of the Act.[52]

4.63 The ALRC makes a number of recommendations in this Report to strengthen the Commissioner's ability to foster and secure compliance in the first instance, monitor compliance as an on-going concern, and enforce compliance where required.

Securing compliance

4.64 The Privacy Commissioner is currently empowered under the *Privacy Act* to give advice, undertake education programs and issue guidelines and other forms of guidance to help agencies and organisations comply with the privacy principles and the objects underlying these principles. The ALRC supports these current functions, and recommends that certain functions be amended to be expressed as broadly as possible.

4.65 The ALRC particularly supports the critical role of the Privacy Commissioner to provide guidance, consistent with the third part of the ALRC's regulatory approach. Guidance can be provided in a variety of forms. One of the most obvious is through guidelines issued by the Privacy Commissioner. Guidance can be provided in information available on the regulator's website, through frequently-asked-questions (FAQs), information sheets, advice, a telephone hotline for enquiries, education programs and tips for compliance. As well as prescribing positive steps for compliance, guidance can be phrased in the negative and set out what will *not* be sufficient in order to achieve compliance with a principle. For example, guidance on the 'Data Security' principle could state that the application of a user name and password is not considered adequate security.

4.66 The Privacy Commissioner has a number of functions that empower him or her to provide guidance to agencies and organisations. These include the functions to: promote an understanding and acceptance of the privacy principles and the objects of those principles;[53] prepare guidelines for the avoidance of acts that might be

---

51 See Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), 3.

52 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 531.

53 *Privacy Act 1988* (Cth) s 27(1)(d).

interferences with privacy or have adverse effects on privacy;[54] provide advice to an agency, organisation or a minister on any matter relevant to the operation of the Act;[55] and undertake education programs for the purpose of promoting the protection of individual privacy.[56] These functions and powers are discussed in detail in Chapter 47.

4.67 A technique suggested by Parker to foster compliance is to encourage the growth of 'compliance professionals' and to promote communication between the compliance professionals and the regulator. Parker has suggested that 'an emerging compliance profession can act as a medium of [a] regulatory community if regulators are willing to engage with them and can also act as a pool of compliance expertise that can be translated into corporate compliance capacity'.[57]

4.68 The ALRC recognises the emergence of the 'privacy professional' in recent years, and the increasing profile of 'privacy officers' in the organisational hierarchy.[58] The OPC should continue to support the growth of privacy professionals and networks such as Privacy Contact Officers and Privacy Connections. Consistent dialogue between the regulator and regulated can help build a 'culture' of privacy, by integrating compliance into organisational practice and developing a shared understanding of the objectives of the *Privacy Act*.[59] A strong relationship between the regulator and regulated entities can also provide a constant update on compliance levels in industries, and can provide more 'intelligence' into how compliance programs are working, how determinations are being received, and other issues. It also provides support to privacy officers in their respective entities, in being able to promote proper privacy practices and engage top levels of management in making privacy compliance a priority.

Monitoring compliance

4.69 Monitoring for compliance is an important part of administering a principles-based regime such as the *Privacy Act*. It recognises that agencies and organisations can decide the steps they will take to achieve the outcome set by the principle, and it provides an avenue for the regulator to assess whether those steps are adequate in an educational, non-confrontational and facilitative way.

---

54 Ibid s 27(1)(e).

55 Ibid s 27(1)(f).

56 Ibid s 27(1)(m).

57 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 555.

58 The growing prominence of privacy officers within corporations was noted in International Association of Privacy Professionals, 'Ponemon Institute, IAPP Announce Results of Annual Salary Survey' (Press Release, 11 March 2005).

59 The ALRC notes the OPC Review's recommendation that it would 'develop strategies for communication with stakeholders, including establishing a privacy contact officer network for private sector organisations': 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 50.

4.70 The ALRC recommends in Chapter 47 that the Commissioner's existing powers to monitor compliance be expanded with the addition of a power to conduct a Privacy Performance Assessment of organisations, in addition to the Commissioner's existing powers to audit in the public sector. Monitoring can and should be used as a proactive tool to secure compliance and to ensure that compliance has been restored after an incident of non-compliance.

Enforcing compliance

4.71 In relation to enforcing compliance, the ALRC strongly supports the enforcement pyramid approach to regulating the *Privacy Act*, and makes several recommendations in Part F to widen the range of strategies that are available to the OPC to enforce compliance with the *Privacy Act*.

4.72 It is important that the OPC adopt a compliance-oriented approach in applying these strategies. While it is consistent with compliance-oriented regulation—and principles-based regulation—to focus initially on restoring compliance through negotiated outcomes (such as conciliation), the OPC should not confine itself to this approach. In particular, the ALRC notes Parker's suggestion that a compliance-oriented regulatory design must incorporate enforcement, 'otherwise, regulators cannot meaningfully and discriminately apply incentives, persuasion, and cooperation to organisations that are complying or attempting in good faith to comply'.[60] As Black suggests, enforcement can play a pivotal role in providing 'incentive structures' to promote compliance.[61]

4.73 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'.[62] A clear enforcement policy that outlines what the usual response to a particular type of breach will be and how that response can be mitigated—such as by evidence of a good internal compliance program—can provide incentives for 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 encourages agencies and organisations to keep complying (or at least keep trying to comply), as they will see that non-compliance, combined with no effort to comply, will attract strong sanctions from the regulator.

---

60 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 534.

61 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 8.

62 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.

4.74 Consistent with the compliance-oriented regulatory design underpinning the *Privacy Act*, the ALRC encourages the OPC to implement a compliance policy that adopts an explicit enforcement pyramid approach to restoring compliance and enforcing the *Privacy Act*. If the OPC is using, and is being seen to be using, a wide range of strategies to ensure compliance with the *Privacy Act*, the benefits of specific and general deterrence that can be generated by a transparent, balanced and vigorous enforcement approach can be achieved.

Light-touch regulation?

4.75 The issue of enforcement often raises the related issue of 'light-touch regulation'. This term appears to be used to describe a variety of approaches and behaviours, some pertaining to the actual form of regulation, others to the regulator's approach to enforcing the Act.

4.76 'Light-touch' can refer to the impact of the actual form of regulation. A pure form of principles-based legislation can be described as 'light-touch' in the sense that its object is not to regulate by laying down detailed operational rules that an organisation must follow in order to be in compliance with the law. Rather, principles-based legislation steps back and states the outcome the regulator wants the regulated entity to achieve, and generally leaves it up to that entity to determine how it is best suited to achieving that outcome.

4.77 Given the hybrid regulatory model adopted by the ALRC, it is not appropriate to describe the privacy regime as uniformly light-touch. While areas regulated primarily by the model UPPs could be described as relatively light-touch, it is unlikely that the recommended *Privacy (Credit Reporting Information) Regulations* would be similarly described.

4.78 Whether the regime can be described as 'light-touch' does not affect the level of compliance which is to be achieved by regulated entities. That is, a light-touch regime does not mean that an agency or organisation does not have to find a way to the outcome, or that compliance is optional or flexible.

4.79 Similarly, the emphasis on preventing breaches in the first instance does not mean that non-compliance with the law will be tolerated and punitive sanctions will not follow a breach. 'Light-touch' does not necessarily mean 'soft-touch' in the compliance response of the regulator, nor does it mean that Parliament intended that the *Privacy Act* not be enforced or that non-compliance be tolerated.

4.80 While compliance-oriented regulation emphasises attempts to restore or nurture compliance through voluntary and conciliatory methods, this merely is the *preferred* approach; it is not the only approach. In some instances, the nature of the breach may be so serious and the behaviour so egregious that a punishment-oriented response—such as seeking civil penalties—will be considered appropriate.

4.81 Alternatively, 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 principle. In such circumstances, the appropriate enforcement response may be to prescribe the steps the respondent should take to achieve compliance with the principle. A principles-based regime does not mean that agencies and organisations will always be left to find their own way to achieving compliance with the principle after an instance of non-compliance.

Scope for co-regulation

Part IIIAA privacy codes

4.82 The ALRC's approach to regulating privacy retains the ability of organisations and industries to flesh out the requirements of the privacy principles in privacy codes approved by the Privacy Commissioner under Part IIIAA.[63]

4.83 This scope for co-regulation is consistent with the overall hybrid approach adopted by the ALRC in its regulatory model. In this model, the legislation establishes the general principles, which then operate 'as the minimum benchmarks or safeguards that must apply across the board'.[64] A code can then sit below the principles and set out the steps that an organisation should take in order to achieve the outcome set by the principles.

4.84 As noted above, within the model of responsive regulation supported by the ALRC, there is an important place for using regulatory tools which conceive non-state actors as 'important regulators in their own right'.[65] While the ALRC understands, to date, that the code-making provisions have not proved popular with industry as a whole, the provisions provide for an important measure of co-regulation which may gain favour in the future as a means of addressing new and developing technologies, and other international concerns.

Codes in regulations

4.85 The ALRC's recommended regulatory model also has the flexibility to accommodate industry-developed codes that derogate from the UPPs. These codes 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, such industry codes would need to obtain the approval of the relevant minister who would then pass the requirements in the codes as regulations, using the ALRC's recommendation regulation-making power.

---

63 Part IIIAA privacy codes are discussed in Ch 48.

64 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 17.

65 J Braithwaite 'Responsive Regulation and Developing Economies' (2006) 34(5) *World Development* 884, 888.

4.86 This is similar to the approach adopted in Part IVB of the *Trade Practices Act 1974* (Cth). Under the *Trade Practices Act*, the Minister has the power to prescribe an industry code of conduct in the regulations.[66] The regulations declare the industry code to be a mandatory industry code or a voluntary industry code, with the former binding on all industry participants.[67] The Act makes the codes enforceable by prohibiting a corporation, in trade or commerce, from contravening an applicable industry code.[68] In the privacy regime, the codes would be enforceable because a breach of the code would constitute an interference with privacy of an individual.

4.87 In the *Trade Practices Act* regime, formal proposals for industry codes are initiated at the ministerial level, 'following representations from industry participants, consumers or government authorities about problems in a particular industry'.[69] It is expected that a similar initiation would take place in the privacy regime, with industry participants lobbying the relevant minister to pass a code in the regulations.

4.88 Being a legislative instrument, the minister must undertake appropriate consultation before making the instrument, which would include ensuring that 'persons likely to be affected by the proposed instrument had an adequate opportunity to comment on its proposed content'.[70] This obligation would ensure that industry views are sought in making the code, and that other bodies—such as the OPC and consumer groups—are also consulted.

Binding Corporate Rules

4.89 Binding Corporate Rules (BCRs) are part of a new framework for regulating privacy in the information age, proposed by the Privacy and Trust Partnership (PTP).[71]

4.90 Under the PTP's proposed framework set out in the Working Paper *A Possible Way Forward: Some Themes and an Initial Proposal for a Privacy and Trust Framework*, the privacy principles would remain the benchmark but 'organisations would be able to vary the principles for their own circumstances'[72] by drafting BCRs to replace the default privacy principles. The PTP explains that any variations in the principles incorporated in a BCR that 'might be perceived as a weakening would need to be compensated for by the variations in other principles *and* by the surrounding

66 *Trade Practices Act 1974* (Cth) pt IVB.
67 Ibid s 51AE.
68 Ibid s 51AD.
69 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.
70 *Legislative Instruments Act 2003* (Cth) s 17(2)(b).
71 See Privacy and Trust Partnership, *A Possible Way Forward: Some Themes and an Initial Proposal for a Privacy and Trust Framework* (2007). The Privacy Trust Partnership is a consortium of businesses, consisting of Veda Advantage Limited, Axciom, IBM, SAS, Suncorp and Microsoft.
72 See Ibid, 11.

compliance, accountability and enforcement framework'.[73] While the PTP suggests that this proposal is similar to Part IIIAA privacy codes, the ALRC notes that the current code provisions (as well as the ALRC's recommended code provisions) do not permit a code to be approved if it weakens a privacy principle.

4.91 While the ALRC understands that this proposal is still being developed, it is useful to note that some aspects of BCRs potentially could be accommodated in the ALRC's recommended regulatory approach. If the BCR derogated from the UPPs, such as by weakening a privacy principle, it would need to be put into regulations, using the ALRC's recommended regulation-making power. The ALRC recognises that having to use the regulation-making power may significantly reduce the flexibility and ease with which BCRs can be changed, which is seen as one of the primary advantages of BCRs. A BCR, however, could not be approved as a code under Part IIIAA, as a code applies in addition to the principles and cannot derogate from them.

4.92 If a BCR was put into regulations, as part of the regulation-making process, the organisation would have to convince the relevant bodies, as well as the general public, that the BCRs were in the public interest and that the BCRs were consistent with the objects of the *Privacy Act*, if not with all the privacy principles.

Summary: Interaction of regulatory tools

4.93 In summary, the basic premise of the ALRC's regulatory approach is that the privacy principles will provide the primary obligations in relation to privacy. The principles will be high-level, technology-neutral and generally non-prescriptive, thereby capable of application to all agencies and organisations subject to the *Privacy Act*. These obligations can, however, be modified or displaced in certain circumstances, including where regulations are passed, a public interest determination is made, or a rule is approved.

4.94 Therefore, the 'privacy obligations' that will apply to an agency or organisation will depend on the agency or organisation in question. Most entities will be regulated entirely by the privacy principles, with an option to refer to (voluntary) guidance issued by the OPC where the agency or organisation desires further detail or advice.

4.95 Agencies and organisations operating in industries where more prescriptive regulation has been deemed necessary—such as credit reporting and health—will be subject to the privacy principles and to any further rules specified in the regulations. In addition, they will have the option of referring to voluntary guidance where they want further assistance.

---

73 See Ibid, 11. Emphasis in original.

4.96 Industries that desire more certainty in how to comply with the principles may decide to embellish on the privacy principles by developing a privacy code to be approved by the Privacy Commissioner. Pursuant to the ALRC's recommended model, such a privacy code would not derogate from the principles and would operate in addition to the principles to prescribe steps on how the organisation should apply or comply with one or more principles. The ALRC's recommended regulatory model, however, will also have the flexibility to accommodate Binding Corporate Rules and codes that are incorporated into regulations.

5. The *Privacy Act*: Name, Structure and Objects

Contents

Introduction

5.1 This chapter provides an overview of the *Privacy Act 1988* (Cth) in its current form and recommends some changes to the name, structure and objects of the Act. It is recommended that the Act be redrafted to achieve greater logical consistency, simplicity and clarity, that an objects clause be included, and that the name of the Act be changed to reflect more accurately the scope of the legislation.

5.2 The Privacy Bill 1988 was introduced into the Australian Parliament in November 1988[1] by the then Attorney-General, the Hon Lionel Bowen MP. The Bill

1 A predecessor Privacy Bill was introduced into Parliament in 1986, in association with the Australia Card Bill 1986, but both Bills lapsed with the double dissolution of Parliament in 1987. The Australia Card proposal is discussed further in Ch 30.

was in part a response to a number of developments in the 1970s and 1980s including continuing advances in the technology available for processing information.

5.3 The Preamble to the Bill makes clear that the legislation was intended to implement Australia's obligations relating to privacy under the United Nations *International Covenant on Civil and Political Rights*[2] (ICCPR) as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[3] (OECD Guidelines). The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*[4] (Council of Europe Convention).

5.4 The Hon Justice Michael Kirby chaired the group of government experts that developed the OECD Guidelines. As Chairman of the Australian Law Reform Commission (ALRC), Justice Kirby also oversaw the production of the three volume Report, *Privacy* (ALRC 22), published in 1983.[5] The Report included draft legislation, which drew on the OECD Guidelines, and was considered by the Australian Government in developing the Privacy Bill.

5.5 The *Privacy Act*, in its original form, set out the Information Privacy Principles (IPPs), which regulate the handling of personal information by Australian Government departments and agencies. It established the position of the Privacy Commissioner, within the Human Rights and Equal Opportunity Commission. The Act provided guidelines for the handling of individual tax file number (TFN) information in both the public and private sectors following enhancements in the use of this identifier in 1988.[6]

5.6 The *Privacy Act* also applies to ACT public sector agencies. In 1994, as part of the transition to self-government, the ACT public service was established as a separate entity from the Australian Government public service. Amendments were made at that time to ensure that ACT public sector agencies continued to be covered by the Act.[7]

5.7 The Act has been substantially amended on a number of occasions. In 1990, the Act was amended to provide safeguards for individuals in relation to consumer credit reporting.[8] These amendments governed the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers.

---

2 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

3 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

4 *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).

5 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

6 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth). TFNs are discussed further in Ch 30.

7 *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).

8 *Privacy Amendment Act 1990* (Cth). Credit reporting is discussed in detail in Part G.

5.8 In 2000, the Act was amended to extend coverage to private sector organisations more generally.[9] This amendment introduced the National Privacy Principles (NPPs) into the legislation. The NPPs were developed following consultation with business, consumers and other stakeholders.[10] Further amendments in 2000 established the Office of the Privacy Commissioner (OPC) as a statutory authority independent of the Human Rights and Equal Opportunity Commission.[11]

Overview of the *Privacy Act*

Agencies and organisations

5.9 Broadly speaking, the IPPs regulate the activities of Australian Government public sector agencies. 'Agency' is defined to include ministers, departments, federal courts and other bodies established for a public purpose.[12] The NPPs regulate the activities of private sector organisations. 'Organisation' is defined as an individual, a body corporate, a partnership, any other unincorporated association or a trust.[13] There are a number of exceptions to, and exemptions from, the definitions of 'agency' and 'organisation'.[14]

Acts and practices

5.10 The *Privacy Act* applies to 'acts and practices', that is, acts done and practices engaged in by agencies or organisations. The Act includes a wide range of exemptions for particular acts and practices discussed briefly below and in more detail in Part E.

5.11 For the purposes of this Report, the ALRC distinguishes between the terms 'handling' and 'processing' of personal information. The ALRC uses the term *handling* personal information to refer to all acts and practices in the information cycle including collection, use, disclosure, storage and destruction of personal information no matter what mechanism is used. The ALRC uses the term *processing* to refer to electronic processing of personal information. The ALRC notes that the European Union Article 29 Data Protection Working Party has drawn the same distinction in its *Opinion 4/2007 on the Concept of Personal Data*.[15]

---

9 *Privacy Amendment (Private Sector) Act 2000* (Cth).

10 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).

11 *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* (Cth).

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

13 Ibid s 6C.

14 Exceptions and exemptions to the *Privacy Act* are discussed in detail in Part E.

15 European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP136 (2007), 5.

Exemptions and exceptions

5.12 The *Privacy Act* contains a range of exemptions and exceptions. They are found throughout the Act, in the definitions of some terms, in specific exemption provisions, and in the IPPs and NPPs themselves. This Report distinguishes between exemptions and partial exemptions to the requirements set out in the 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 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 Act; or some or all of the provisions of the Act, but only in relation to certain of its activities. For example, the federal courts are *partially exempt* as they only are required to comply with the Act in relation to their administrative 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. These distinctions are discussed in more detail in Chapter 33.

5.13 The acts and practices of some Australian Government agencies—including the intelligence agencies: the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation and the Office of National Assessments—are completely exempt from the *Privacy Act*.[16]

5.14 Certain acts and practices of other agencies are also exempt. For example, while federal courts fall within the definition of agency for the purposes of the *Privacy Act*, only some acts and practices of federal courts are covered by the Act.[17] Acts and practices in relation to administrative functions such as personnel files, operational and financial records, and mailing lists, for example, are covered.[18] However, acts done and practices engaged in as part of the courts' judicial functions are not covered.

5.15 In relation to the private sector, the definition of organisation specifically excludes many small business operators and registered political parties. Small businesses are defined in the *Privacy Act* as those with an annual turnover of $3 million or less. This exemption was included in order to avoid the imposition of unjustified compliance costs on small business.[19] Some small businesses that pose a higher risk to privacy—for example, small businesses that hold health information and provide health services or those that trade in personal information—are covered by the Act.[20] Other small business operators may choose to opt in to the regime[21] or may be brought into the regime by regulation.[22]

---

16 *Privacy Act 1988* (Cth) s 7. This issue is discussed in detail in Ch 34.
17 Ibid s 7. This issue is discussed in detail in Ch 35.
18 *I v Commonwealth Agency* [2005] PrivCmrA 6.
19 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General). This issue is discussed in detail in Ch 39.
20 *Privacy Act 1988* (Cth) s 6D(4).
21 Ibid s 6EA.
22 Ibid s 6E.

5.16 State and territory public sector authorities fall outside the definition of 'agency' and are specifically excluded from the definition of 'organisation'. States and territories may request, however, that such authorities be brought into the regime by regulation.[23]

5.17 The *Privacy Act* does not apply to personal information being collected, used or disclosed for personal, family or household purposes.[24]

5.18 The *Privacy Act* includes an exemption for employee records. Organisations are exempt in relation to past or present employees if the relevant act or practice is directly related to an employee record and the employment relationship.[25] At the time the private sector amendments were passed, the Attorney-General noted that this type of personal information was deserving of privacy protection but that the issue was more appropriately dealt with in workplace relations legislation.[26] To date, however, the issue has not been effectively dealt with in this way and so employee records in the private sector remain without adequate privacy protection.

5.19 Media organisations are exempt in relation to acts or practices in the course of journalism.[27] A media organisation is an organisation whose activities consist of or include the collection, preparation and dissemination of news, current affairs, information or documentaries. Media organisations can claim the exemption if they have publicly committed to observing published, written standards that deal with privacy in the context of media activities. This exemption is intended to allow a free flow of information to the public through the media.[28]

5.20 Political acts and practices by political representatives, such as parliamentarians, are exempt where those acts and practices relate to the political process. Contractors, subcontractors and volunteers working for registered political parties or political representatives also may be exempt where their acts or practices are related to the political process.[29]

5.21 The IPPs and NPPs include a number of exceptions. For example, under IPP 6 individuals are entitled to access their own personal information except to the extent that a record-keeper is required or authorised by or under law to refuse to provide the individual with access. IPP 10 provides that personal information shall not be used for

---

23 Ibid s 6F.
24 Ibid ss 7B(1), 16E. This issue is discussed in Ch 11.
25 Ibid s 7B(3). This issue is discussed in detail in Ch 40.
26 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
27 *Privacy Act 1988* (Cth) s 7B(4).
28 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General). This issue is discussed in detail in Ch 42.
29 *Privacy Act 1988* (Cth) s 7C. This issue is discussed in detail in Ch 41.

any purpose other than the purpose for which it was collected. This principle is subject to specified exceptions, for example, where the use of the information for that other purpose is: necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; required or authorised by or under law; or necessary to enforce the criminal law. There are similar exceptions relating to the disclosure of personal information under IPP 11.

5.22 The NPPs contain a range of similar exceptions as well as specific and qualified exceptions for the use of non-sensitive information for direct marketing purposes[30] and the use of health information for research, or the compilation or analysis of statistics, relevant to public health or public safety.[31]

Information Privacy Principles

5.23 The 11 IPPs are based on the OECD Guidelines.[32] The IPPs are a central feature of the *Privacy Act* and are discussed in detail in Part D. The IPPs require that Australian Government agencies have a lawful purpose for collecting personal information, and that the purpose is related to the functions or activities of the agency.[33] An agency collecting personal information from an individual must ensure that: that individual is generally aware of the purpose for which the information is being collected; whether the collection is authorised or required by or under law; and the agency's usual practices in relation to disclosure of such information.[34] The IPPs require agencies to ensure that information is relevant, up-to-date and complete.[35]

5.24 Agencies must also store information securely[36] and provide information about the type of personal information they hold.[37] Subject to certain exceptions, agencies must provide individuals with access to personal information about them and correct the information they hold to ensure that it is accurate, up-to-date, relevant, complete and not misleading.[38] Agencies must generally seek an individual's permission to use or disclose information for a purpose that is not directly related to the purpose for which it was collected.[39]

National Privacy Principles

5.25 The 10 NPPs—developed in consultation with private sector organisations—apply in the private sector where no approved privacy code has been put in place.[40] The

30 Ibid sch 3, NPP 2.1(c).
31 Ibid sch 3, NPP 2.1(d).
32 Ibid s 14.
33 Ibid s 14, IPP 1.
34 Ibid s 14, IPP 2.
35 Ibid s 14, IPP 3.
36 Ibid s 14, IPP 4.
37 Ibid s 14, IPP 5.
38 Ibid s 14, IPP 7.
39 Ibid s 14, IPPs 10, 11.
40 Ibid sch 3.

NPPs are discussed in detail in Part D. The NPPs require that organisations collect personal information by lawful and fair means and not in an unreasonably intrusive manner. The information must be necessary for one of the organisation's functions or activities and must be collected from the individual concerned, where it is reasonable and practicable to do so.[41] Sensitive information, including health information, may only be collected with consent except in specified circumstances.[42]

5.26 Organisations may only use and disclose personal information for the purpose for which it was collected, except in a number of defined circumstances. For example, an organisation may use personal information for a related purpose if that would be within the reasonable expectations of the individual.[43] Organisations must take reasonable steps to ensure that the personal information they handle is accurate, complete and up-to-date,[44] and must protect the information from misuse and loss and from unauthorised access, modification or disclosure.[45] Organisations must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.[46]

5.27 On request, organisations are required to let individuals know what sort of personal information they hold and how they handle that information,[47] and to give individuals access to the information held about them unless particular exceptions apply.[48] There are limits on the use of government identifiers by the private sector,[49] and on transferring personal information overseas.[50] Organisations are also required to have a written privacy policy, which sets out how the organisation manages personal information, and to make the policy available to anyone who asks for it.[51]

Approved privacy codes

5.28 The *Privacy Amendment (Private Sector) Act 2000* (Cth) introduced Part IIIAA into the *Privacy Act*, which allows private sector organisations and industries to develop and enforce their own privacy codes. Once the Privacy Commissioner approves a privacy code, it replaces the NPPs for those organisations bound by the code.[52] Codes may also set out procedures for making and dealing with complaints.

41 Ibid sch 3, NPP 1.
42 Ibid sch 3, NPP 10.
43 Ibid sch 3, NPP 2.
44 Ibid sch 3, NPP 3.
45 Ibid sch 3, NPP 4.
46 Ibid sch 3, NPP 4.
47 Ibid sch 3, NPP 5.
48 Ibid sch 3, NPP 6.
49 Ibid sch 3, NPP 7.
50 Ibid sch 3, NPP 9.
51 Ibid sch 3, NPP 5.
52 Ibid s 16A.

Such codes must provide for the appointment of an independent adjudicator to whom complaints may be made.[53]

5.29 The aim of amending the Act in this way was to encourage private sector organisations and industries to develop privacy codes of practice.[54] To date, only four codes have been approved by the Privacy Commissioner: the Market and Social Research Privacy Code, the Queensland Club Industry Privacy Code, the Biometrics Institute Privacy Code and the General Insurance Information Privacy Code. The General Insurance Information Privacy Code has since been revoked. Privacy codes are discussed further in Chapter 48.

Interference with privacy

5.30 Part III Division 1 of the *Privacy Act* sets out what amounts to an 'interference with privacy', that is, a breach of the Act that gives grounds for a complaint to the Privacy Commissioner or an independent adjudicator appointed under an approved privacy code. An act or practice by an agency that breaches an IPP is an interference with privacy.[55] An act or practice by an organisation that breaches an NPP or an approved privacy code is an interference with privacy.[56] An interference with privacy may also arise in other areas including: credit reporting, the handling of TFN information, and data-matching.

Credit reporting

5.31 As noted above, the *Privacy Act* was amended in 1990—following public controversy over the credit industry's intention to introduce a system of 'positive' (more comprehensive) credit reporting[57]—to provide safeguards for individuals in relation to consumer credit reporting.[58] In particular, Part IIIA of the Act regulates the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers. The Privacy Commissioner is required to issue a Code of Conduct that, together with Part IIIA, applies privacy protections to the handling of personal credit information.[59] The current Code includes amendments

53 Ibid s 18BB.
54 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
55 *Privacy Act 1988* (Cth) s 13.
56 Ibid s 13A.
57 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) <www.privacy.gov.au> at 14 April 2008.
58 *Privacy Amendment Act 1990* (Cth).
59 *Privacy Act 1988* (Cth) s 28A.

made following a number of reviews.[60] The credit reporting provisions have been the subject of criticism[61] and are considered in detail in Part G.

Tax file numbers

5.32 TFNs are unique numbers issued by the Australian Taxation Office (ATO) to identify individuals, companies and others who lodge income tax returns with the ATO. The *Privacy Act* provides for the making of specific guidelines in relation to the collection, storage, use and security of TFN information relating to individuals.[62] The TFN Guidelines, issued under s 17 of the *Privacy Act*, are legally binding. A breach of the guidelines is an interference with privacy and provides grounds for a complaint to the Privacy Commissioner.[63] Interim Guidelines contained in a schedule to the *Privacy Act* operated until they were replaced with the *Tax File Number Guidelines 1990*. The current guidelines were issued in 1992 and have been amended on a number of occasions.[64]

Privacy Commissioner

5.33 The *Privacy Act* establishes the position of the Privacy Commissioner as an independent statutory officer who is appointed by the Governor-General for a period of up to seven years.[65] The powers and role of the Privacy Commissioner are examined in detail in Part F.

Office of the Privacy Commissioner

5.34 The *Privacy Act* establishes the OPC—consisting of the Privacy Commissioner and his or her staff—as a statutory agency to oversee the implementation of the *Privacy Act*.[66] The Office consists of the following sections:

- the Executive Unit;
- the Compliance section;
- the Policy section; and
- the Corporate and Public Affairs section.

---

60 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) <www.privacy.gov.au> at 14 April 2008.

61 See, eg, G Greenleaf, 'The Most Restrictive Credit Reference Laws in the Western World?' (1992) 66 *Australian Law Journal* 672; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.11].

62 TFNs are discussed in detail in Ch 30.

63 Unauthorised use or disclosure of TFNs is also an offence under the *Taxation Administration Act 1953* (Cth). This Act protects all TFNs and not just those of individuals.

64 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).

65 *Privacy Act 1988* (Cth) ss 19–25.

66 Ibid ss 19, 26A.

5.35 The Executive Unit comprises the Privacy Commissioner, Deputy Commissioner, Assistant Commissioner and staff.

5.36 The Compliance section investigates complaints from individuals about agencies and organisations. It also investigates possible breaches of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and associated Guidelines, the TFN Guidelines, and the guidelines in force under the *National Health Act 1953* (Cth). In addition, the section audits agencies, credit providers and credit reporting agencies. Compliance also conducts audits under s 309 of the *Telecommunications Act 1997* (Cth). The Enquiries Line is located in the Compliance section and provides assistance to individuals in relation to their rights under the *Privacy Act* and related legislation. It also provides advice to agencies and organisations on how to comply with the Act and related legislation.

5.37 The Policy section provides guidance and advice to agencies and organisations on privacy issues; examines and makes submissions on proposed legislation; comments on inquiries that have significant privacy implications; and seeks to keep up-to-date on technological and social developments that affect individual privacy. The Corporate and Public Affairs section assists the OPC in communicating with stakeholders through publications, media relations, speech writing, events and the OPC website.[67]

Functions of the Privacy Commissioner

5.38 The Privacy Commissioner's functions are set out in a number of Acts including the *Privacy Act*. Those in the *Privacy Act* include:

- promoting an understanding and acceptance of the IPPs and the NPPs and undertaking educational programs in relation to privacy;
- investigating acts or practices that may breach the IPPs or NPPs, either in response to complaints or on the Commissioner's own initiative;
- auditing the handling of personal information by agencies to ensure that they comply with the IPPs;
- considering and approving privacy codes and reviewing the operation of the codes and decisions of adjudicators appointed under those codes;
- considering legislation that might impact on privacy and ensuring that any adverse effects are minimised;

67 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 14 April 2008.

- undertaking research into and monitoring developments in data processing and computer technology to ensure that any adverse privacy effects of such developments are minimised;

- publishing various guidelines, including binding guidelines, on the development of privacy codes and the use of health information for medical research;[68] and

- providing advice to the Minister and others.[69]

5.39 As noted above, the Privacy Commissioner also has functions under the *Privacy Act* in relation to TFN information and credit reporting. In addition, the Commissioner has responsibilities under the:

- *Data-matching Program (Assistance and Tax) Act 1990* (Cth) in regulating the conduct of Australian Government data-matching programs. The Privacy Commissioner is required to issue guidelines under the Act and has the power to investigate acts or practices that may breach the guidelines;[70]

- *National Health Act 1953* (Cth) in regulating the handling of Medicare and Pharmaceutical Benefits Program claims information. The Privacy Commissioner is required to issue guidelines under the Act and has the power to investigate acts or practices that may breach the guidelines;[71]

- *Crimes Act 1914* (Cth) in regulating the handling of information about spent convictions. Part VIIC of the Act provides for a spent convictions scheme that prevents discrimination against individuals on the basis of certain previous convictions. The Commissioner has the power to investigate complaints about breaches of Part VIIC;[72] and

- *Telecommunications Act 1997* (Cth) in monitoring disclosures of personal information to law enforcement agencies and consulting on industry codes and standards in a range of consumer protection and privacy areas.[73]

5.40 In performing his or her functions, the Privacy Commissioner is required to take certain matters into account, including Australia's international obligations and

---

68 The guidelines made under ss 95 and 95A of the *Privacy Act* in relation to the use of health information in research are discussed in Ch 64.

69 *Privacy Act 1988* (Cth) s 27.

70 These guidelines are discussed further in Chs 10 and 47.

71 These guidelines are discussed further in Chs 47 and 61.

72 These functions are discussed further in Ch 47.

73 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 14 April 2008. These functions are discussed further in Ch 71.

relevant international guidelines on privacy. The Commissioner is also required to have due regard to the protection of important human rights and social interests that compete with privacy such as the free flow of information through the media and the right of government and business to achieve their objectives in an efficient way.[74]

Investigations

5.41 The Privacy Commissioner has the power to investigate—on his or her own motion, or in response to a complaint—acts and practices of agencies or organisations that may breach the IPPs or NPPs.[75] In conducting such investigations, the Commissioner can require the production of documents and information, and may also require people to appear and answer questions.[76] The Commissioner may examine such witnesses on oath or affirmation.[77]

5.42 The Privacy Commissioner may make a determination where there has been a breach of the IPPs or NPPs.[78] The Commissioner may determine that the conduct must not be repeated; that the agency or organisation must take action to redress the loss or damage caused; or that the complainant is entitled to a specified amount of compensation. The Commissioner also may dismiss the complaint or decide to take no further action. Such determinations, however, are not binding as between the parties. If it becomes necessary to enforce the determination, action must be taken in the Federal Court or the Federal Magistrates Court.[79]

Public Interest Determinations

5.43 The Privacy Commissioner has the power to make Public Interest Determinations (PIDs) and Temporary Public Interest Determinations (TPIDs) that exempt certain acts and practices from the operation of the Act, where they would otherwise be a breach of the IPPs or NPPs.[80] The Commissioner may issue a PID where he or she is satisfied that the public interest in an agency or organisation doing an act or engaging in a practice substantially outweighs the public interest in adhering to the IPPs or NPPs. The Privacy Commissioner may make a TPID, in limited circumstances, where an application for a PID contains matters of an urgent nature.

---

74 *Privacy Act 1988* (Cth) s 29.
75 Ibid pt V.
76 Ibid s 44.
77 Ibid s 45.
78 Ibid s 52.
79 Ibid s 55A.
80 Ibid ss 72, 80A and 80B.

5.44 The Privacy Commissioner has made 10 PIDs to date. PIDs and TPIDs are disallowable instruments under the *Legislative Instruments Act 2003* (Cth). They must be tabled in the Australian Parliament and are then subject to disallowance.[81]

Privacy Advisory Committee

5.45 The *Privacy Act* provides for the establishment of a Privacy Advisory Committee made up of the Privacy Commissioner and not more than six other members.[82] The Act requires that members of the Advisory Committee have a range of expertise, for example, in industry or public administration, the trade union movement, electronic data processing, social welfare and civil liberties.[83]

5.46 The Advisory Committee is intended to provide high-level strategic advice to the Privacy Commissioner and, subject to any direction by the Commissioner, to engage in community education and consultation.[84]

Privacy regulations

5.47 Section 100(1) of the *Privacy Act* provides that:

> The Governor-General may make regulations, not inconsistent with this Act, prescribing matters:
>
> (a) required or permitted by this Act to be prescribed; or
>
> (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

5.48 Various other provisions in the Act also provide for the making of regulations. Section 6(5C), for example, states that the regulations may provide that businesses or undertakings of a specified kind are not credit reporting businesses within the meaning of the Act. Section 6E provides that the regulations may prescribe certain small business operators to be organisations for the purposes of the Act. Section 6F provides that the regulations may prescribe certain state and territory authorities and instrumentalities to be organisations for the purposes of the Act.

---

81 Ibid ss 80 and 80C. These provisions both refer to s 46A of the *Acts Interpretation Act 1901* (Cth). That provision has been repealed. Section 6(d)(i) of the *Legislative Instruments Act 2003* (Cth) provides that instruments declared to be disallowable instruments for the purposes of s 46A of the *Acts Interpretation Act* should be deemed legislative instruments for the purposes of the *Legislative Instruments Act*.

82 Ibid s 82. The Privacy Advisory Committee is discussed further in Ch 46.

83 The current members of the Advisory Committee are Peter Coroneos, Chief Executive Officer, Internet Industry Association; Associate Professor John M O'Brien, School of Organisation and Management, University of New South Wales; Suzanne Pigdon, former Privacy and Customer Advocacy Manager, Coles Myer Group; Dr William Pring, Director of Consultation-Liaison, Psychiatry Services, Box Hill Hospital; Joan Sheedy, Assistant Secretary, Privacy and FOI Policy Branch, Department of the Prime Minister and Cabinet; and Robin Banks, Chief Executive Officer, Public Interest Advocacy Centre Ltd and Director, Public Interest Law Clearing House Inc.

84 *Privacy Act 1988* (Cth) s 83.

5.49 In Chapter 54, the ALRC recommends that the provisions dealing with credit reporting be promulgated as regulations under the *Privacy Act*.[85] In Chapter 60, the ALRC recommends that the provisions dealing specifically with the handling of health information be promulgated as regulations under the Act.[86] Both these sets of regulations are intended to modify the operation of the model Unified Privacy Principles (UPPs)—discussed in detail in Part D—in relation to credit reporting information and health information respectively.

5.50 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72),[87] the ALRC proposed that the *Privacy Act* should be amended to provide for the making of regulations that modify the operation of the UPPs to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations than are provided for in the UPPs.[88] This proposal was based on the view that such modifications can be consistent with the *Privacy Act*—and with the objects of the *Privacy Act* recommended below[89]—even where they impose less stringent requirements on agencies and organisations than those imposed by the UPPs. For example, it may be necessary to modify the operation of the UPPs in order to achieve an appropriate balance between the public interest in protecting the privacy of individuals with other public interests, such as allowing important public health research to proceed.

Submissions and consultations

5.51 The OPC did not support this proposal. The OPC was concerned that the proposed regulation-making power seemed to envisage the making of regulations that would be inconsistent with the *Privacy Act*. The Office was of the view that the regulation-making power should continue to be modified by the phrase 'not inconsistent with this Act'. The OPC also expressed concern about allowing statutory protections to be modified by regulation, and noted that the Australian Government *Legislation Handbook* provides that rules that have a significant impact on individual rights and liberties should be implemented through Acts of Parliament.[90]

5.52 Telstra stated that:

> There are two major concerns with this proposal. First, regulations are not the most appropriate mechanism for modifying primary legislation in this way. Under the proposal, the regulations will contain substantial obligations inconsistent with the *Privacy Act*. Regulations are delegated legislation and disallowable instruments, not legislation, and it is inappropriate for regulations to significantly modify primary legislation passed by the Parliament.

---

85 Rec 54–1.
86 Rec 60–1.
87 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007).
88 Ibid, Proposal 3–1.
89 Rec 5–4.
90 Australian Government Department of the Prime Minister and Cabinet, *Legislation Handbook* (1999), [1.12].

> Second, regulations are capable of being changed relatively easily, which gives rise to a concern that there will be insufficient checks and balances applicable to the process of changing the privacy regime governing some of these specific industries. Given the significance of the industry specific regulatory regime, it should be dealt with through primary legislation and only changed by an amending Act.[91]

5.53 The Australian Bankers' Association (ABA) was also concerned that the proposal may result in ongoing changes to compliance obligations.[92]

5.54 The Office of the Victorian Privacy Commissioner (OVPC), and a number of other stakeholders, did not support allowing the regulations to impose less stringent requirements than the UPPs.[93] The Public Interest Advocacy Centre (PIAC) noted that:

> PIAC is concerned that such an approach may lead to a gradual erosion of privacy protection through subordinate legislation as has happened in New South Wales. In recent years, the NSW Government has gradually watered down the *Privacy and Personal Information Protection Act 1998* (NSW) through successive regulations and other statutory instruments, sometimes without consulting the Privacy Commissioner.[94]

5.55 A number of stakeholders also stated that allowing the UPPs to be modified by regulation might undermine the aim of harmonisation or create unnecessary complexity.[95] The OVPC noted that any such regulations will need to be replicated in state and territory legislation in order to maintain national consistency.[96]

5.56 On the other hand, Microsoft Asia Pacific noted that the *Legislative Instruments Act* requires consultation where practicable and appropriate before the making of regulations and other legislative instruments. This is particularly the case where the regulations are likely to have a direct or substantial indirect effect on business.[97] Microsoft Asia Pacific expressed the view that this would

> help to ensure that proposed regulations have no unintended consequences, and that they are an appropriate and effective means of regulating the particular context in which they are intended to apply.[98]

---

91 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
92 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.
93 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
94 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
95 Confidential, *Submission PR 570*, 13 February 2008; Government of South Australia, *Submission PR 565*, 29 January 2008; Confidential, *Submission PR 536*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.
96 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
97 *Legislative Instruments Act 2003* (Cth) s 17.
98 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

5.57 Google Australia also supported the proposal in principle submitting that:

> A flexible approach to regulation is essential in a landscape where technology is developing at a pace that is quicker than the capacity for legislation to address the challenges posed by new technologies.[99]

5.58 The Australian Government Department of Human Services expressed support for the proposal, but noted that a similar outcome could be achieved more easily and with the same level of legal certainty, oversight and transparency using other forms of legislative instrument, rather than regulations. The department did not indicate, however, what form of instrument would be appropriate.[100] The Australian Privacy Foundation also supported the proposal in principle, but noted that any derogation from the UPPs should be 'positively affirmed' by the Australian Parliament rather than left to the discretion of the Privacy Commissioner.[101] Other stakeholders expressed unqualified support for the proposal.[102]

ALRC's view

5.59 The ALRC did not propose, and is not recommending, a regulation-making power that is inconsistent with the *Privacy Act*. The ALRC is recommending a regulation-making power that allows modifications to be made to the UPPs. In the ALRC's view, such modifications can be consistent with the *Privacy Act*, even where they impose less stringent requirements than the UPPs on agencies and organisations. The ALRC agrees with the OPC that the regulation-making power should continue to be modified by the phrase 'not inconsistent with this Act' and has included this qualification in the recommendation below.

5.60 The ALRC notes, in addition, that the Australian Government *Legislation Handbook* states that matters subject to frequent change and other matters may be included in subordinate legislation in order to streamline primary legislation. The ALRC has recommended that amendments to the UPPs relevant only to health information, for example, be included in the new *Privacy (Health Information) Regulations* for these reasons.[103] This regulatory framework will allow the UPPs to remain as streamlined as possible, while providing flexibility to adapt the UPPs where necessary in particular contexts.

5.61 The Act should make clear that the regulations may modify the operation of the UPPs to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations

---

99 Google Australia, *Submission PR 539*, 21 December 2007.

100 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

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

102 GE Money Australia, *Submission PR 537*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

103 Australian Government Department of the Prime Minister and Cabinet, *Legislation Handbook* (1999), [6.45]–[6.46].

than are provided for in the UPPs. The Privacy Commissioner may currently modify the operation of the IPPs and NPPs by making a Public Interest Determination (PID). PIDs are issued on the basis that the public interest in a particular act or practice outweighs the public interest in maintaining the level of protection provided by the IPPs or NPPs. This means that a PID may put in place a regime which imposes different or more specific requirements in particular contexts, including imposing less stringent requirements on agencies and organisations than are provided for in the IPPs and NPPs. The Privacy Commissioner should retain the power to issue PIDs.[104] In developing regulations that would modify the application of the UPPs, similar issues would have to be considered in order to ensure that the regulations were consistent with the *Privacy Act*.

5.62 In Chapter 3, the ALRC recommends that the Australian Government and state and territory governments establish an intergovernmental cooperative scheme under which each state and territory would enact legislation regulating the handling of personal information in that state or territory's public sector. Such legislation would apply the UPPs, any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act*.[105] To promote and maintain uniformity across the jurisdictions, the ALRC also recommends that the Standing Committee of Attorneys-General (SCAG) should develop an intergovernmental agreement to ensure that any proposed changes to these key elements must be approved by SCAG and, where relevant, the Australian Health Ministers' Conference.[106] Any regulations enacted that would amend the UPPs would have to be considered and approved in this way.

Recommendation 5–1 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 model Unified Privacy Principles (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.

The structure of the Act

5.63 Because the *Privacy Act* has been substantially amended on a number of occasions, the numbering and structure of the Act make it confusing and difficult to navigate. For example, while the IPPs are found in s 14 of the Act, the NPPs are found in Schedule 3. In addition, the Act refers to obsolete legislation such as the

104 See Ch 47.
105 Rec 3–4.
106 Rec 3–5.

Conciliation and Arbitration Act 1904 (Cth) and to provisions such as s 46A of the *Acts Interpretation Act 1901* (Cth) that have been repealed and replaced.

5.64 As discussed above, and in Parts D and E of this Report, exemptions and exceptions are found throughout the Act and, in some cases, in other pieces of legislation. This can make it difficult to ascertain whether the *Privacy Act* covers a particular agency or organisation and, if so, to what extent. In addition, the drafting of some exemptions, such as exempt acts and practices in s 7, is complex and difficult to understand.

5.65 In the course of the Inquiry, a significant number of stakeholders commented on the problems caused by the complex structure of the *Privacy Act*.[107] Electronic Frontiers Australia expressed the view that the Act was 'complex, confusing and unwieldy' and that this was leading to misapplication of the provisions.[108] The Centre for Law and Genetics agreed that the Act has become difficult to work with:

> We would strongly support the redrafting of the legislation to achieve a greater degree of simplicity and clarity. Nevertheless, the original flow from collection through to release arose from the OECD Guidelines and this remains a defensible template.[109]

5.66 The Office of the Information Commissioner Northern Territory was of the view that the *Privacy Act* had 'lost its way' and should be redrafted, using plain English, and restructured, including grouping exemptions together.[110] Privacy NSW agreed.[111] A number of commentators have also been critical of the Act's complexity.[112]

Discussion Paper proposal

5.67 In DP 72, the ALRC expressed the view that such complexity seems undesirable in legislation intended to protect individuals' personal information. An individual is unlikely to be able to take action to protect his or her rights if it is difficult to ascertain what acts and practices of agencies and organisations are covered by the legislation.

---

107 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 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; AAMI, *Submission PR 147*, 29 January 2007; 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; W Caelli, *Submission PR 99*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Tasmanian Ombudsman, *Consultation PC 158*, Hobart, 30 March 2007.

108 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

109 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

110 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

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

112 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, [6.1]; 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).

The ALRC proposed that the *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity, including the consolidation of the IPPs and the NPPs into a single set of UPPs; the clarification and grouping together of exemptions; and the restructuring and renumbering of the Act.[113]

Submissions and consultations

5.68 There was strong support for this proposal.[114] PIAC noted that:

> The Act is well overdue for a complete overhaul. In its current form, it lacks coherence, and is overly complex and confusing. Many of PIAC's clients have complained that they have been unable to understand their rights from their own reading of the Act and have therefore been put in the position of being forced to seek legal advice and representation. This is inappropriate in a jurisdiction that encourages self-representation.[115]

5.69 The Australian Government Department of Human Services expressed support for the proposal, but noted that substantial changes to the *Privacy Act* will present more difficulties for agencies than for organisations, and that training will be required to manage the transition.[116]

5.70 Several stakeholders expressed concern about the proposal, however, drawing attention to the significant investment that has been made to establish policies and procedures to meet the requirements of the current regime. These stakeholders noted that any major reform of the Act will come at a cost as agencies and organisations will be required to amend policies and procedures to meet new requirements.[117]

---

113 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–2.

114 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; BPay, *Submission PR 566*, 31 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; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Google Australia, *Submission PR 539*, 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; 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; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; National Transport Commission, *Submission PR 416*, 7 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Mortgage and Finance Association of Australia, *Submission PR 344*, 19 November 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

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

116 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

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

ALRC's view

5.71 The ALRC acknowledges that there will be costs involved for agencies and organisations in updating policies and procedures to meet new requirements imposed by an amended *Privacy Act*. In the ALRC's view, however, the current complexity is giving rise to ongoing and significant costs and that these costs cannot be justified into the future. These issues are discussed in detail in Chapter 14.

5.72 In Chapter 18, the ALRC recommends the introduction of a single set of UPPs applying to both agencies and organisations.[118] This change, alone, would resolve much of the complexity in the current provisions. In Chapter 33, the ALRC also recommends that the exemptions in the *Privacy Act* should be clarified and located together.[119] Amending the *Privacy Act* in line with these recommendations would provide an excellent opportunity to restructure the entire Act to achieve greater logical consistency, simplicity and clarity.

Recommendation 5–2 The *Privacy Act* should be redrafted to achieve greater logical consistency, simplicity and clarity.

The name of the Act

5.73 The *Privacy Act* is essentially limited in its scope to the protection of personal information. It does not regulate other elements of the right to privacy, for example, the right to be free from arbitrary or unlawful interference with one's home or family life. The Privacy Commissioner, Karen Curtis, noted in evidence to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry):

> I think we should all remember that, while our *Privacy Act* is about the protection of personal information or sensitive information, it is really about data protection. It is not about privacy in the broader sense of bodily privacy or privacy in other areas. I think 'privacy' is often seen as a catch-all and so our *Privacy Act* does not address all aspects of territorial privacy or bodily privacy.[120]

5.74 The Australian Government is not alone in using this nomenclature for legislation that protects personal information. Both Canada and New Zealand have a Privacy Act. The Canadian *Privacy Act 1985* regulates the handling of personal information by the public sector. The New Zealand *Privacy Act 1993* regulates the handling of personal information in both the public and the private sector.

---

118 Rec 18–2.
119 Rec 33–1.
120 Commonwealth, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 51 (K Curtis—Privacy Commissioner).

5.75 Names given to similar legislation in a number of other jurisdictions, however, indicate more accurately the scope of the legislation; for example:

- *Privacy and Personal Information Protection Act 1998* (NSW);
- *Information Privacy Act 2000* (Vic);
- *Personal Information Protection Act 2004* (Tas);
- *Information Act 2002* (NT);
- *Data Protection Act 1998* (United Kingdom); and
- *Personal Information Protection and Electronic Documents Act 2000* (Canada).[121]

5.76 Nomenclature in the legislative context is important because accurate descriptive names provide a snapshot of the content of the legislation. Names may also serve political purposes, for example, assisting the passage of a Bill through Parliament, and may act to publicise the legislation locally and internationally.[122] Names that do not accurately describe the scope of legislation may mislead the public into believing that a law covers particular areas that, in fact, it does not.

5.77 In DP 72, the ALRC proposed that the *Privacy Act* should be renamed the *Privacy and Personal Information Act* on the basis that the current name does not accurately reflect the main focus of the legislation, and has the potential to cause confusion.[123] This is a particular problem with a term such as 'privacy', which potentially covers a number of areas and is in general use in the community in relation to matters that are not covered by the *Privacy Act*. The ALRC suggested that the proposed name more clearly reflected the main focus of the Act, that is, the privacy of personal information, while at the same time being wide enough to indicate that the Privacy Commissioner has a number of functions that do not relate to personal information.

5.78 Alternatively, if the Act were amended to include a statutory cause of action for invasion of privacy, as proposed in DP 72,[124] the ALRC suggested that the name of the Act should remain the same.

---

121 The *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) regulates the handling of personal information by the private sector.

122 M Whisner, 'What's in a Statute Name?' (2005) 97 *Law Library Journal* 169, 183.

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

124 Ibid, Proposal 5–1.

Submissions and consultations

5.79 A number of submissions expressed support for the current name of the *Privacy Act*.[125] The OPC noted that the functions of the Privacy Commissioner set out in s 27 of the Act are wider than the protection of personal information. They include education to promote the protection of individual privacy[126] and recommendations to the Attorney-General on the need for legislative or administrative action in the interests of privacy.[127]

> Moreover, the Office observes that information privacy can intersect with other categories of privacy. For example, location detection technologies, which collect information about an individual's whereabouts, might be considered to cut across both information and physical privacy. In the view of the Office, the *Privacy Act* should therefore continue to be an instrument that can effectively respond to these broader privacy issues.[128]

5.80 The OPC suggested that the Act should be renamed the *Australian Privacy Act* to differentiate it more clearly from privacy legislation in other jurisdictions. The OPC was of the view that the ALRC's proposed title, the *Privacy and Personal Information Act*, was similar to the New South Wales *Privacy and Personal Information Protection Act* and had the potential to cause confusion. The OPC stated that the *Australian Privacy Act* would be appropriate, whether or not the Act was amended to include a statutory cause of action for invasion of privacy. In the alternative, the OPC submitted that the current name, the *Privacy Act*, provides clear and simple branding that differentiates the legislation from privacy legislation in the states and territories.[129]

5.81 On the other hand, there was considerable support for renaming the legislation to focus more expressly on the protection of personal information. The OVPC commented that:

> The inclusion of 'Privacy' in the title of the IPA [*Information Privacy Act 2000* (Vic)] and its national and interstate equivalents, has, in my experience, created confusion on the part of enquirers and complainants. Many of those who contact my office are seeking information or assistance about matters outside of the jurisdiction of the IPA, including bodily and spatial privacy. If these matters remain outside of the coverage of the *Privacy Act*, then its name should be changed to reflect this.[130]

---

125 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.

126 *Privacy Act 1988* (Cth) s 27(1)(m).

127 Ibid s 27(1)(r).

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

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

130 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

5.82 Alternative names suggested by stakeholders included:

- Information Privacy Act;[131]
- Personal Information Privacy Act;[132]
- Personal Information Privacy Protection Act;[133]
- Personal Information Regulation Act;[134]
- Protection of Personal Information Act;[135]
- Privacy and Information Protection Act;[136]
- Data Protection Act;[137] and
- Privacy and Data Protection Act.[138]

5.83 A number of stakeholders expressly supported the use of the term 'data' in the name of the legislation.[139] The Australian Direct Marketing Association noted that this would be in keeping with the European privacy information regime and the emerging Asia-Pacific Economic Cooperation (APEC) regime. In the Association's view, adopting this terminology would be more accurate and would assist global consistency and recognition of Australian law.[140]

5.84 The Australian Privacy Foundation, however, did not support the use of the name Data Protection Act, put forward by a number of stakeholders, because it might

---

131 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Law Institute of Victoria, *Submission PR 200*, 21 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; Veda Advantage, *Submission PR 163*, 31 January 2007; L Bygrave, *Submission PR 92*, 15 January 2007.

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

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

134 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

135 Confidential, *Submission PR 143*, 24 January 2007.

136 National Association for Information Destruction, *Submission PR 133*, 19 January 2007.

137 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; National Association for the Visual Arts, *Submission PR 151*, 30 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

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

139 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

imply that the legislation was limited to computerised information or was only concerned about security.[141]

5.85 The PIAC stated that it:

> does not support the proposal that the Act should be renamed the *Privacy and Personal Information Act* as this suggests that the legislation is about personal information generally, when it is actually about the protection of such information. PIAC does agree, however, that it is important to retain the term 'privacy' in the title of the Act, as some of the functions of the Privacy Commissioner go beyond data protection. The use of this term also helps to maintain a rights-based context for the legislation. In PIAC's view, a preferable name for the Act would be the *Personal Information Privacy Protection Act*.[142]

5.86 A number of stakeholders supported the ALRC's proposed change.[143] Other stakeholders expressed support for this option as well as the alternative option of leaving the name unchanged if the Act is amended to include a statutory cause of action for invasion of privacy.[144]

ALRC's view

5.87 If the *Privacy Act* is not amended to include a statutory cause of action, for the reasons stated above, the Act should be renamed the *Privacy and Personal Information Act*. This name reflects more clearly the main focus of the Act, that is, the privacy of personal information, while at the same time being wide enough to indicate that the Privacy Commissioner has a number of functions that do not relate to personal information.

5.88 The ALRC has considered the OPC's suggestion that the Act should be renamed the Australian Privacy Act, however, this proposed title would not accurately reflect the scope of the legislation and that including the term 'Australian' in the title is not necessary. 'Australian' is often included in the title of legislation at the national level where it forms part of the name of the organisation established by the legislation, for example, *Australian Law Reform Commission Act 1996* (Cth). Where this is not the case, the relevant jurisdiction is traditionally indicated by a bracketed abbreviation following the name of legislation: *Privacy Act 1988* (Cth). This avoids the need to include the word 'Australian' in the name of all federal legislation.

5.89 In Chapter 74, the ALRC recommends that federal legislation provide for a statutory cause of action for invasion of privacy.[145] The statutory cause of action would

---

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

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

143 Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.

144 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

145 Rec 74–1.

arise in a range of situations, including where there has been an interference with an individual's home or family life, an individual has been subjected to unauthorised surveillance, or an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed. While the ALRC has not expressly recommended that the statutory cause of action be included in the *Privacy Act*, it logically could be located there. If the *Privacy Act* is amended in this way, the name of the Act should remain the same.

Recommendation 5–3 The *Privacy Act* should be renamed the *Privacy and Personal Information Act*. If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, however, the name of the Act should remain the same.

The objects of the Act

5.90 An objects clause is a provision—often located at the beginning of a piece of legislation—that outlines the underlying purposes of the legislation and can be used to resolve uncertainty and ambiguity. Objects clauses have been described as a 'modern day variant on the use of a preamble to indicate the intended purpose of legislation'.[146] The Office of Parliamentary Counsel, which is responsible for drafting Australian Government legislation, has noted that:

> Some objects provisions give a general understanding of the purpose of the legislation … Other objects provisions set out general aims or principles that help the reader to interpret the detailed provisions of the legislation.[147]

5.91 Objects clauses may assist the courts and others in the interpretation of legislation.[148] Section 15AA of the *Acts Interpretation Act 1901* (Cth) states that:

> In the interpretation of a provision of an Act, a construction that would promote the purpose or object underlying the Act (whether that purpose or object is expressly stated in the Act or not) shall be preferred to a construction that would not promote that purpose or object.

146 D Pearce and R Geddes, *Statutory Interpretation in Australia* (6th ed, 2006), 154.
147 Office of Parliamentary Counsel, *Working with the Office of Parliamentary Counsel: A Guide for Clients* (3rd ed, 2008), [125].
148 See, eg, *Tickner v Bropho* (1993) 114 ALR 409.

5.92 The interpretation statutes of the states and territories contain similar or identical provisions.[149] Cole JA of the New South Wales Court of Appeal has made clear that

> whilst regard may be had to an objects clause to resolve uncertainty or ambiguity, the objects clause does not control clear statutory language, or command a particular outcome of exercise of discretionary power.[150]

5.93 The *Privacy Act* does not include a section setting out the objects of the legislation. The Act does include a Preamble, however, that indicates that the legislation is intended to give effect to Australia's obligations in relation to privacy under the ICCPR and to implement the OECD Guidelines.

5.94 A number of other federal Acts in the field of human rights—including the *Sex Discrimination Act 1984* (Cth), the *Disability Discrimination Act 1992* (Cth) and the *Age Discrimination Act 2004* (Cth)—include an objects clause. Recent federal statutes containing an objects clause include the *Airspace Act 2007* (Cth), the *National Greenhouse and Energy Reporting Act 2007* (Cth) and the *Northern Territory National Emergency Response Act 2007* (Cth).

International instruments

5.95 A number of international instruments dealing with privacy set out their aims and objects. The Preface to the OECD Guidelines states in part that

> although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.[151]

5.96 Article 1 of 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:

> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.[152]

---

149 *Interpretation Act 1987* (NSW) s 33; *Interpretation of Legislation Act 1984* (Vic) s 35(a); *Acts Interpretation Act 1954* (Qld) s 14A; *Interpretation Act 1984* (WA) s 18; *Acts Interpretation Act 1915* (SA) s 22; *Acts Interpretation Act 1931* (Tas) s 8A; *Interpretation Act 1978* (NT) s 62A.

150 *Minister for Urban Affairs and Planning v Rosemount Estates Pty Ltd* (1996) 91 LGERA 31, 78.

151 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Preface.

152 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 1 Objects of the Directive.

5.97 The Preamble to the APEC Privacy Framework states that:

> Finally, this Framework on information privacy protection was developed in recognition of the importance of:
>
> - Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
> - Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;
> - Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
> - Enabling enforcement agencies to fulfill their mandate to protect information privacy; and
> - Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.[153]

Federal privacy legislation

5.98 Although the *Privacy Act* does not include an objects clause, s 29 of the Act requires the Privacy Commissioner to have regard to a number of matters in performing his or her functions. These include the protection of important human rights and social interests that compete with privacy such as the general desirability of a free flow of information, through the media and otherwise, and the right of government and business to achieve their objectives in an efficient way.[154] The Commissioner is also required to take into account Australia's international obligations, including those concerning communications technology, and international guidelines relevant to the better protection of individual privacy.[155] The Commissioner must also ensure that his or her recommendations and guidelines are, within the limitations of the powers of the Commonwealth, capable of acceptance, adaptation and extension throughout Australia.[156]

5.99 Section 3 of the *Privacy Amendment (Private Sector) Act* states that the main objects of that Act are:

> (a) to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the

153 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Preamble.
154 *Privacy Act 1988* (Cth) s 29(a).
155 Ibid s 29(b).
156 Ibid s 29(c).

appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations; and

(b) to do so in a way that:

(i) meets international concerns and Australia's international obligations relating to privacy; and

(ii) recognises individuals' interests in protecting their privacy; and

(iii) recognises 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 right of business to achieve its objectives efficiently.

State and territory privacy legislation

5.100 The *Information Privacy Act 2000* (Vic),[157] the *Information Act 2002* (NT)[158] and the Information Privacy Bill (WA)[159] expressly set out their objects. The *Privacy and Personal Information Protection Act 1998* (NSW) and the *Personal Information Protection Act 2004* (Tas), however, do not include an objects clause.

5.101 Section 5 of the Victorian *Information Privacy Act* provides that the objects of that Act are:

(a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;

(b) to promote awareness of responsible personal information handling practices in the public sector;

(c) to promote the responsible and transparent handling of personal information in the public sector.

Submissions and consultations

General comments

5.102 There was significant support for amending the *Privacy Act* to include an objects clause,[160] although a small number of stakeholders expressed the view that an objects clause was unnecessary.[161]

---

157 *Information Privacy Act 2000* (Vic) s 5.

158 *Information Act 2002* (NT) s 3.

159 Information Privacy Bill 2007 (WA) cl 3.

160 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Law Institute of Victoria, *Submission PR 200*, 21 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; National Association for Information Destruction, *Submission PR 133*, 19 January 2007; Centre for Law

5.103 The Office of the Information Commissioner Northern Territory stated that:

> I consider that the impact of the privacy principles could be significantly enhanced by a brief statement of the overarching objects to guide those who must interpret and implement them. This could either appear as an introductory statement to the principles or as an objects clause at the start of the Act.[162]

5.104 The National Health and Medical Research Council (NHMRC) suggested that an objects clause would assist health service providers, researchers and others to understand the overall purpose, structure and direction of the legislation and, on that basis, better interpret and apply the legislation.[163] The OVPC noted that the objects set out in s 5 of the *Information Privacy Act* had been extremely useful. The Office suggested that:

> In the interests of national consistency, it would be desirable for the objects of state and territory privacy legislation to be amended or drafted to align, to the maximum extent possible, with the objects of the *Privacy Act*. This should of course occur by way of consultation between the Commonwealth and state and territory governments.[164]

5.105 Stakeholders suggested that the objects of the *Privacy Act* might include:

- to balance the public interest in protecting individual privacy with other public interests;[165]
- to secure the right of individuals to control the dissemination of information about their own lives;[166]
- to promote the responsible and transparent handling of personal information;[167]
- to protect the information privacy of individuals while authorising appropriate uses of their personal information;[168]

---

and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

161 Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Telstra Corporation Limited, *Submission PR 459,* 11 December 2007.

162 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

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

164 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

165 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

166 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

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

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

- to achieve national consistency;[169] and
- the matters set out in s 29 of the *Privacy Act*, discussed above.[170]

Comments on specific elements of the proposed objects clause

5.106 In DP 72, the ALRC proposed that the legislation should include an objects clause and that those objects should be to:

(a) implement Australia's obligations at international law in relation to privacy;

(b) promote the protection of individual privacy;

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;

(d) establish a cause of action to protect the interests that individuals have in the personal sphere free from interference from others;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic commerce, nationally and internationally, while ensuring respect for the right to privacy; and

(g) provide the basis for nationally consistent regulation of privacy.[171]

5.107 While there was significant support for the ALRC's proposed objects clause,[172] stakeholders made the following comments in relation to individual elements.

---

169 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

170 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

171 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–4.

172 Government of South Australia, *Submission PR 565*, 29 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; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Transport Commission, *Submission PR 416*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; D Hall, *Submission PR 372*, 4 December 2007.

(a) Implement Australia's obligations at international law in relation to privacy

5.108 Telstra did not support the inclusion of an objects clause and, in addition, was of the view that this paragraph was too wide and appeared to be intended to incorporate all international norms relating to privacy into Australian law.[173]

(b) Promote the protection of individual privacy

5.109 The Australian Privacy Foundation was of the view that paragraph (b) should come first in the list of objects.[174] The OPC suggested amending paragraph (b) to refer explicitly to the individual's right to privacy.[175] The Arts Law Centre of Australia expressed the view that paragraph (b) should read 'to promote the protection of personal information' rather than 'to promote the protection of individual privacy' to more accurately reflect the scope of the legislation. This was on the basis that the Centre did not support the inclusion of a statutory cause of action for invasion of privacy in the *Privacy Act*.[176]

(c) Recognise that the right to privacy is not absolute and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests

5.110 The ABA expressed the view that this proposed paragraph was uncertain and should be clarified by way of example. The ABA suggested that the objects clause should include recognition of the desirability of the free flow of information and the right of government and business to achieve their objectives in an efficient way.[177] A number of other stakeholders also expressed the view that the objects clause should recognise the importance of freedom of expression and the general desirability of the free flow of information[178] or appropriate information sharing.[179] The Arts Law Centre of Australia was of the view that proposed paragraph (c) should make clear that privacy does not take precedence over other human rights.[180] Other arts organisations agreed.[181]

---

173 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
174 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
175 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
176 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.
177 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.
178 Special Broadcasting Service, *Submission PR 530*, 21 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.
179 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.
180 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.
181 Contemporary Arts Organisations Australia, *Submission PR 384*, 6 December 2007; Artsource, *Submission PR 350*, 28 November 2007.

5.111 PIAC expressed concern about paragraph (c) on the basis that the paragraph appeared to reduce the right to privacy to a public interest 'that can readily be traded off against other public interests'. In the Centre's view, the provision should recognise that the right to privacy is not absolute, but that the appropriate balance is between the right to privacy and other human rights and freedoms.[182]

5.112 The OPC did not support proposed paragraph (c) and expressed the view that it was not consistent with art 17 of the ICCPR.[183] The OPC suggested, as an alternative, that one of the objects of the legislation should be to

> recognise that the right to privacy is not absolute and to provide a framework within which agencies and organisations may conduct their legitimate functions and activities in a manner that respects individuals' right to privacy.[184]

5.113 In the OPC's view, the notion of balancing interests overlooks the situations in which good privacy practice supports the objectives of agencies and organisations. The OPC noted that privacy is not always in competition with other public interests but may advance those interests.[185]

(d) Establish a cause of action to protect the interests that individuals have in the personal sphere free from interference from others

5.114 The Arts Law Centre of Australia and a number of other stakeholders did not support a statutory cause of action and, as a consequence, did not support including this element in the objects clause.[186] In addition, Telstra expressed the view that the clause was expressed too broadly and was likely to lead to an interpretation of the proposed cause of action that went beyond privacy to include such issues as personality rights.[187]

(f) Facilitate the growth and development of electronic commerce, nationally and internationally, while ensuring respect for the right to privacy

5.115 PIAC did not support including this element in the objects clause stating that 'it is inappropriate to import into what is essentially human rights legislation an objective to facilitate the growth and development of electronic commerce'.[188]

5.116 The Australian Government Attorney-General's Department noted that the *Electronic Transactions Act 1999* (Cth) includes an objects clause that makes clear that

---

182 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
183 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).
184 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
185 Ibid.
186 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.
187 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
188 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

the Act is intended is to provide a regulatory framework that: recognises the importance of the information economy to the future economic and social prosperity of Australia; facilitates the use of electronic transactions; promotes business and community confidence in the use of electronic transactions; and enables business and community to use electronic communications in their dealings with government.[189]

New objects

5.117 The OPC suggested the addition of several new elements to the objects clause. These were the establishment of the position of the Privacy Commissioner and the OPC, and the provision of 'a means for addressing complaints about an alleged interference with an individuals' information privacy'.[190]

ALRC's view

5.118 The *Privacy Act* would benefit from the inclusion of an objects clause setting out the purpose and aims of the legislation. This is particularly important in principles-based legislation, because principles require constant interpretation and application to particular contexts and an objects clause provides a reference framework to assist with this.

5.119 Some of the matters set out in s 29 of the *Privacy Act* for consideration by the Privacy Commissioner in carrying out his or her functions would sit more appropriately in an objects clause. These matters are relevant to the interpretation and application of the Act by all stakeholders, not only the Privacy Commissioner.

5.120 The ALRC recommends that the objects clause include the following elements. The clause should state that one of the objects of the Act is to implement, in part, Australia's obligations at international law in relation to privacy. This provides a pointer to relevant international instruments and jurisprudence that may assist in interpreting and applying the legislation. The ALRC acknowledges Telstra's concern that, if the statutory cause of action is not included in the *Privacy Act*, the legislation will only partially implement Australia's international obligations in relation to privacy and has amended the recommended wording accordingly.

5.121 The clause should also state that the Act is intended to recognise that individuals have a right to privacy and to promote the protection of that right. The ALRC agrees with the OPC that the objects clause should make express reference to the right to privacy. The right to privacy is one of a number of fundamental human rights set out in the ICCPR and other international instruments and, while the right is not absolute, one of the objects of the *Privacy Act* should be to promote protection of that right.

---

189 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
190 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

5.122 Chapter 1 discusses how the right to privacy competes, collides and coexists with other rights and interests, such as freedom of expression. The objects clause should acknowledge these tensions. It should make clear that the Act is intended to recognise that the right to privacy is not absolute and provide a framework within which to balance that right with other human rights. It should also reflect the need to balance the public interest in protecting the privacy of individuals with other public interests.

5.123 This formulation recognises that rights should be balanced with rights and public interests with public interests. Although the right to privacy is an individual right, there is a strong public interest in protecting that right. For example, it is essential that health consumers are confident that their health information will be handled appropriately or they may resist sharing that information with health service providers. This has the potential to have a negative impact on the health of the individual and is also an undesirable public policy outcome, with the potential to impact on the health of the community as a whole.

5.124 The ALRC does not agree with the OPC's assertion that this element is inconsistent with art 17 of the ICCPR. The United Nations Human Rights Committee has stated in relation to art 17 that:

> As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant.

5.125 This clearly envisages a balancing of interests and, in particular, a balancing of public interests. The other human rights that must be balanced with the right to privacy, and the public interests that must be balanced with the public interest in protecting privacy, are many and varied. It is not only the right to freedom of expression[191] that must be considered but numerous other rights including the right to liberty and security of the person,[192] and the right of every child 'to such measures of protection as are required by his status as a minor, on the part of his family, society and the State'.[193] These other rights and public interests should not be expressly set out in the objects clause. A general statement, such as that recommended below, alerts the community to the need to consider the right to privacy in context without placing undue weight on any other particular right or public interest.

5.126 The objects clause should make clear that the Act is intended to provide the basis for nationally consistent regulation of privacy and the handling of personal information across Australia. Chapter 3 sets out the ALRC's recommendations to achieve greater national consistency.

---

191 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19.

192 Ibid, art 9.

193 Ibid, art 24.

5.127 The objects clause should also make clear that the Act is intended to promote the responsible and transparent handling of personal information by agencies and organisations.

5.128 The ALRC also recommends that the objects include facilitating the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy. This clause draws on a number of international instruments that have been developed in this area including the OECD Guidelines, the EU Directive and the APEC Privacy Framework. It recognises that one of the primary issues in this area is the growth and development of electronic transactions and the need to ensure that these transactions are conducted, across Australia and between Australia and other countries, in ways that protect the privacy of individuals' personal information.

5.129 The ALRC agrees with the OPC that the objects clause should also refer to the establishment of the position of the Privacy Commissioner and, in the language of this Report, the Australian Privacy Commission. The ALRC also recommends that the objects clause make reference to the fact that the legislation provides an avenue for individuals to seek redress when there has been an alleged interference with their privacy.

5.130 In DP 72, the ALRC proposed that the cause of action for a serious invasion of privacy be included in the *Privacy Act*.[194] This proposal was reflected in a number of elements of the proposed objects clause. The ALRC's final view, however, is that it is not necessary for the cause of action be included in the Act.[195] On the other hand, if the cause of action were so included, the objects clause would need to be amended to reflect this fact.

Recommendation 5–4 The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be specified to:

(a) implement, in part, Australia's obligations at international law in relation to privacy;

(b) recognise that individuals have a right to privacy and to promote the protection of that right;

194 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 5–1.
195 Rec 74–1.

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests;

(d) provide the basis for nationally consistent regulation of privacy and the handling of personal information;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy;

(g) establish the Australian Privacy Commission and the position of the Privacy Commissioner; and

(h) provide an avenue for individuals to seek redress when there has been an alleged interference with their privacy.

6. The *Privacy Act*: Some Important Definitions

Contents

Introduction

6.1 Part II of the *Privacy Act 1988* (Cth) sets out a number of important definitions. While these will be discussed in detail, where relevant, throughout this Report, some core definitions are discussed below and a number of changes to these definitions are recommended. In particular, the ALRC recommends bringing the definition of 'personal information' more into line with international law and including some biometric information in the definition of 'sensitive information'.

What is 'personal information'?

6.2 Central to the regime established by the *Privacy Act* is the definition of 'personal information'. This is because the privacy principles only apply to personal information as defined by the Act. The current definition of personal information is the same as that found in the original 1988 Act, that is:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[1]

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

6.3 A crucial element in this definition is that personal information must be 'about an individual whose identity is apparent, or can reasonably be ascertained'. In 2002, the then Privacy Commissioner, Malcolm Crompton, stated that:

> An important distinction needs to be made between identity and identification. Identity is a complex, multifaceted notion. Each of us has a range of different identities defined through relations with others, position, status, actions, behaviours, characteristics, attitudes and the circumstances of the moment …
>
> Identification is the action of being identified, of linking specific information with a particular person. An individual's identity has a degree of fluidity and is likely to change over time. The extensive linking of different information about an individual may restrict or limit this fluidity …
>
> Identification can potentially relate a wide range of elements of an individual's identity. In practice, identifying an individual generally involves focusing on those things that distinguish that individual from others including, legal name, date of birth, location or address and symbolic identifiers such as a driver's licence number.[2]

6.4 A number of submissions to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (the Senate Committee privacy inquiry) suggested that the definition of personal information in the Act needed to be updated to deal with new technologies and new methods of collecting information.[3] Research done on behalf of the Consultative Committee of the Council of Europe Convention highlighted that new technology makes it possible to process data relating to individuals—and to develop profiles of those individuals—that are not linked to their legal identity such as their name and address.[4]

6.5 The Office of the Privacy Commissioner (OPC) has stated that:

> The definition of personal information provides latitude for the Office to take into consideration contextual factors when determining if information should be subject to the *Privacy Act*. These contextual factors go to determining whether an individual's identity is 'readily ascertainable'.
>
> The Office recognises the challenges posed by the development of new technologies and processes, particularly in the field of data-matching, that have the potential to create identified information from data sources containing previously anonymous data. However, the definition of personal information leaves open the flexibility to

---

2 M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002).

3 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.19]–[3.24]; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005; Centre for Law and Genetics, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 February 2005.

4 Y Poullet, *Report on the Application of Data Protection Principles to the Worldwide Telecommunications Networks* (2004) Council of Europe, 33.

> consider the degree to which an organisation is able to 'reasonably ascertain' someone's identity, including by the use of such technologies.[5]

6.6 Both the OPC review of the private sector provisions of the *Privacy Act* (the OPC Review) and the Senate Committee privacy inquiry recommended that the ALRC, in its review of the *Privacy Act*, examine the definition of 'personal information' and any amendments to the definition that may be needed to reflect technological advances and international developments in privacy law.[6]

International instruments

6.7 The Oganisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Guidelines)[7] and the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (the Council of Europe Convention)[8] define 'personal data' as 'any information relating to an identified or identifiable individual'. The European Parliament *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* (the EU Directive) defines 'personal data' as 'any information relating to an identified or identifiable natural person' and goes on to say that an identifiable person is

> one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[9]

6.8 The European Union Article 29 Data Protection Working Party has stated that:

> At this point, it should be noted that, while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other 'identifiers' are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her … the individual's contact point (a computer) no longer necessarily

---

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

6 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 7.15; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 69.

7 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), art 1.

8 *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), art 2.

9 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 2.

> requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects this fact.[10]

6.9 The Asia-Pacific Economic Cooperation *Privacy Framework* (the APEC Privacy Framework) defines 'personal information' as 'any information about an identified or identifiable individual'. The Framework goes on to state that this includes information that can be used to identify an individual, as well as information that would not meet this criteria alone, but when put together with other information would identify an individual.[11]

Other jurisdictions

6.10 A 2004 report on the meaning of 'personal data', prepared for the United Kingdom Information Commissioner, examined the definition and application of the term in the privacy legislation of 18 countries. The report found that there is 'no one uncontested and coherent definition' of 'personal data'.[12]

6.11 Both the Canadian *Personal Information Protection and Electronic Documents Act 2000*[13] and the New Zealand *Privacy Act 1993*[14] simply define 'personal information' as 'information about an identifiable individual'.

6.12 The Information Privacy Bill 2007 (WA) defines personal information, in part, as follows:

> Personal information is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead—
>
> (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or
>
> (b) who can be identified by reference to an identifier or an identifying particular such as a fingerprint, retina print or body sample.[15]

6.13 The *Data Protection Act 1998* (UK) states that 'personal data' means:

> data which relate to a living individual who can be identified
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

---

10 European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP136 (2007).

11 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [9].

12 S Booth and others, *What are 'Personal Data'?—A Study Conducted for the UK Information Commissioner* (2004), 8.

13 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 2(1).

14 *Privacy Act 1993* (NZ) s 2.

15 Information Privacy Bill 2007 (WA) cl 6.

> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[16]

6.14 The United Kingdom Information Commissioner has issued detailed legal guidelines on the *Data Protection Act*, including in relation to the meaning of 'personal data':

> An individual is 'identified' if you have distinguished that individual from other members of a group … Simply because you do not know the name of an individual does not mean you cannot identify that individual. Many of us do not know the names of all our neighbours, but we are still able to identify them … There will be circumstances where the data you hold enables you to identify an individual whose name you do not know and you may never intend to discover.[17]

6.15 The Information Commissioner provided the following example:

> Where an individual is not previously known to the operators of a sophisticated multi-camera town centre CCTV system, but the operators are able to distinguish that individual on the basis of physical characteristics, that individual is identified. Therefore, where the operators are tracking a particular individual that they have singled out in some way (perhaps using such physical characteristics) they will be processing 'personal data'.[18]

6.16 In earlier guidance, the Information Commissioner expressed the view that:

> If the information about a particular web user is built up over a period of time, perhaps through the use of tracking technology, with the intention that it may later be linked to a name and address, that information is personal data. Information may be compiled about a particular web user, but there might not be any intention of linking it to a name and address or e-mail address. There might merely be an intention to target that particular user with advertising, or to offer discounts when they re-visit a particular web site, on the basis of the profile built up, without any ability to locate that user in the physical world. The Commissioner takes the view that such information is, nevertheless, personal data. In the context of the on-line world the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others.[19]

6.17 In more recent guidance, however, the Information Commissioner makes clear that data is likely to be personal data where it is linked to an individual and is processed with the intention of determining or influencing the way in which the person is treated, rather than simply distinguishing that person from others.[20]

---

16 *Data Protection Act 1998* (UK) s 1(1).

17 United Kingdom Government Information Commissioner's Office, *Data Protection Technical Guidance: Determining What is Personal Data* (2007).

18 Ibid.

19 United Kingdom Government Information Commissioner's Office, *Data Protection Act 1998 Legal Guidance* (2001), 12.

20 United Kingdom Government Information Commissioner's Office, *Data Protection Technical Guidance: Determining What is Personal Data* (2007).

About an individual

6.18 The current definition in the *Privacy Act* states that information must be 'about an individual'. The APEC Privacy Framework also requires that information be 'about' an individual. On the other hand, the OECD Guidelines, the Council of Europe Convention and the EU Directive require that information 'relate to' an individual.

6.19 The 2004 report prepared for the United Kingdom Information Commissioner notes that not all data that relate to an individual should fall within the definition of 'personal information'. To hold that all information that could affect or be linked to an individual is 'personal information' 'runs the risk of making all data personal data'. The report stated that the limiting factor is that the information must relate to an identifiable individual: the information must either identify the individual or be able to be linked to information that can identify the individual. The report defines this kind of information as being 'about' the individual.[21]

Ability to contact

6.20 Another issue that was raised over the course of the Inquiry was whether the definition of 'personal information' should include information that simply allows an individual to be contacted, such as a stand alone telephone number or Internet Protocol (IP) address. A number of stakeholders suggested that the definition should include information sufficient to allow communications with an individual whether or not it is sufficient to allow the individual to be identified.[22]

Discussion Paper proposals

6.21 In Discussion Paper 72, *Review of Australian Privacy Law* (DP 72),[23] the ALRC proposed bringing the definition of 'personal information' in the *Privacy Act* more in line with the definitions used in relevant international instruments. The ALRC noted the distinction drawn by the former Privacy Commissioner between 'identity' and 'identification', set out above, and expressed the view that the *Privacy Act* should apply to information about an individual who is 'identified or reasonably identifiable' rather than information about an individual whose 'identity' is apparent, or reasonably ascertainable. The ALRC suggested that 'personal information' should be defined as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.[24]

6.22 The ALRC also proposed that the Explanatory Memorandum to the amended *Privacy Act* make clear that an individual is 'reasonably identifiable' when the

---

21 S Booth and others, *What are 'Personal Data'?—A Study Conducted for the UK Information Commissioner* (2004), 11.

22 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

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

24 Ibid, Proposal 3–5(a).

individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.[25] The ALRC proposed that the Privacy Commissioner should issue guidance on the meaning of 'identified or reasonably identifiable'.[26]

6.23 The ALRC did not propose a change to the terminology requiring personal information to be 'about' an individual. Although a number of international instruments use the term 'relates to', the *Privacy Act* terminology is consistent with the APEC Privacy Framework and reflects the fact that the information must be about an identified or reasonably identifiable individual. Finally, the ALRC suggested that information that simply allows an individual to be contacted—such as a stand alone telephone number, street address or IP address—would not, and should not, fall within the proposed definition of 'personal information'. The *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. This broader issue is discussed in Chapter 1 in relation to the meaning of 'privacy'.

Submissions and consultations

General comments

6.24 A number of stakeholders expressed support for the existing definition of 'personal information' in the *Privacy Act*.[27] The Australian Bankers' Association (ABA) noted that changing key definitions in the Act would come at some cost to industry and should only be done if a clear case for change was made out.[28] A number of other stakeholders agreed, suggesting that the current definition was appropriate and noting that any change would result in an unjustified compliance burden.[29] BPAY stated that:

> BPAY believes that the current definition of 'personal information' in the *Privacy Act* is adequate. Without compelling reasons to change the definition, any change to the definition is likely to generate considerable uncertainty, and implementation and compliance costs. These costs may be quite disproportionate to any benefit that may be obtained with respect to the protection of an individual's privacy.[30]

---

25 Ibid, Proposal 3–5(b).

26 Ibid, Proposal 3–5(c).

27 BPay, *Submission PR 566*, 31 January 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; AXA, *Submission PR 119*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.

28 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

29 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Investment and Financial Services Association, *Submission PR 538*, 21 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.

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

6.25 DLA Phillips Fox noted that the current definition is broad enough to capture information in any medium and sufficiently flexible to allow for future technological developments.[31] The OPC agreed with the need to maintain flexibility, noting that:

> The definition of personal information is contingent on context for its application. In the view of the Office, this is one of the strengths of the definition, allowing it to respond to change and technological advance. In order to alleviate any confusion generated by the flexibility of the term, the Office intends to issue further guidance material.[32]

6.26 The OPC, however, along with a significant number of other stakeholders, expressed support for the changes to the definition of 'personal information' proposed in DP 72.[33] Australia Post commented positively on the fact that this would bring the definition more into line with relevant international instruments.[34] There was also support for the proposals to provide guidance on the meaning of 'reasonably identifiable' in the Explanatory Memorandum and in guidelines to be developed and published by the Privacy Commissioner.[35]

An identified or reasonably identifiable individual

6.27 Although there was widespread support for the proposed change to the definition of 'personal information', there were also some concerns expressed. The Australian Privacy Foundation suggested that the test should be whether information is 'potentially identifiable' rather than 'reasonably identifiable'.[36] GE Money Australia was of the view that use of the term 'reasonably' would introduce greater uncertainty and that the meaning of 'personal information' should be left to guidance issued by the Privacy Commissioner.[37]

---

31 DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

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

33 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; School of Public Health—University of Sydney, *Submission PR 504*, 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; Privacy NSW, *Submission PR 468*, 14 December 2007; Australian Library and Information Association, *Submission PR 446*, 10 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Australian Digital Alliance, *Submission PR 422*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

34 Australia Post, *Submission PR 445*, 10 December 2007.

35 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; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; I Graham, *Submission PR 427*, 9 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

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

6.28 On the other hand, while Microsoft Asia Pacific did not support a change to the definition of personal information, it stated that, if the definition was amended along the lines suggested by the ALRC, it was important to retain the 'reasonableness' test:

> This test necessitates a consideration of the cost, difficulty, practicality and likelihood of the organisation linking information with other personal information accessible to it, and not merely whether the organisation would be able to link the information after incurring substantial expenditure ... In Microsoft's experience as a large organisation that handles and processes significant volumes of personal information for its business purposes, it is apparent to us that just because an organisation holds, or is capable of accessing, various pieces of information about an individual, it does not follow that it will always combine this information to ascertain the identity of that individual. In many cases it is not practical or useful for this to be done, and so it simply does not occur.[38]

6.29 A number of other stakeholders did not support the ALRC's proposed definition on the basis that, in the current technological environment, all information held by agencies and organisations is potentially 'identifiable'.[39] Acxiom Australia noted that although it was almost always possible to use technology to link information with identified individuals, that did not mean that agencies or organisations would do so.[40] The Insurance Council of Australia expressed the view that assessing whether an organisation held personal information about individuals who were 'reasonably identifiable', would itself give rise to behaviour that was inconsistent with the objectives of the *Privacy Act*.[41]

6.30 A number of early submissions to the Inquiry had expressed concern that, with the advent of the internet and other technologies—such as location based services including mobile phones and the Global Positioning System (GPS)—it is possible to build profiles of individuals using identifiers such as mobile phone numbers.[42] In DP 72, the ALRC expressed the view that a mobile telephone number, email address or IP address could be, or could become, personal information once that information was linked to a particular individual due to the accretion of information around the number or address. The Australian Compliance Institute expressed support for the proposition that the definition of 'personal information' should capture information such as an email address where it is possible to use the information to target or affect the individual in some way.[43]

---

38 Microsoft Asia Pacific, *Submission PR 463,* 12 December 2007.

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

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

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

42 AAMI, *Submission PR 147,* 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

43 Australasian Compliance Institute, *Submission PR 419,* 7 December 2007.

6.31 The Public Interest Advocacy Centre (PIAC) suggested that:

> There is a need to move away from the concept of identification in defining personal information and to look instead at whether the information enables interactions with an individual on a personalized basis. This is a much more practical and measurable test than whether someone is 'identifiable or reasonably identifiable'.[44]

6.32 The Australian Communications and Media Authority (ACMA) noted that its practice in anti-spam investigations is to treat all email addresses in spam email headers as 'personal information'. However, in relation to IP addresses, ACMA submitted that, as IP addresses uniquely identify computers connected to the internet, they relate to machines and not to individuals using the machines. ACMA did note, however, that while an individual's identity may not be readily apparent from an IP address alone, that identity 'can be ascertained when the IP address is correlated at a given point in time with the IP address data and other data held by the individual's internet service provider'. ACMA expressed concern that uncertainty about when IP addresses become 'personal information' for the purposes of the *Privacy Act* may impair its ability to share such information with overseas authorities in the course of investigative and enforcement actions.[45]

6.33 The Australian Government Attorney-General's Department noted that:

> Clear guidelines are required to establish the point at which telephone numbers, email addresses or IP addresses become personal information. In part these should cover the attributes required to link an individual to an IP address, email address or telephone number and the point at which the aggregation of IP address, email address and phone number may also identify the individual.[46]

6.34 In addition, there was concern expressed about the proposed clarification of the meaning of 'reasonably identifiable' to be included in the Explanatory Memorandum. Several stakeholders supported the approach proposed—that an individual is 'reasonably identifiable' if the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access—but were of the view that such qualifiers should be included in the legislation.[47]

6.35 The Cyberspace Law and Policy Centre expressed support for the proposed definition, agreeing that

> what makes the data 'personal information' is that the individual is treated differently from other individuals because of information which is specific to them, even though their name may not be known to the party which is using the information.[48]

---

44 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
45 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.
46 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
47 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
48 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

6.36 The Centre doubted, however, that the courts would interpret the proposed definition in this way. The Centre was of the view that guidance by the Privacy Commissioner would not be sufficient in these circumstances, and urged that the matter be addressed in the legislation itself, or in the Explanatory Memorandum.[49]

6.37 On the other hand, a number of stakeholders expressed concern about the content of the proposed Explanatory Memorandum clarification.[50] Telstra stated that it would be impossible for an organisation to take into account information that they are 'likely to access' in deciding whether information is 'personal information' for the purposes of the *Privacy Act*. In addition, Telstra stated that:

> The problem with this approach is that it does not seem to require the information to be actually linked or intended to be linked by an organisation for it to fall within the definition. Thus, when an organisation collects information about an individual that does not in itself amount to personal information, it would then be required to investigate what other information about that individual is in the organisation's possession in order to determine whether or not the information is to be treated as personal information, even if it does not, and does not intend to, link those items of information. This would be a mammoth task, particularly for large organisations, and would result in increased compliance costs without any clear additional public benefit.[51]

6.38 The Law Council of Australia queried whether it was necessary to include the clarification in the Explanatory Memorandum, and asked what criteria would be applied to judge whether an organisation is 'likely to access' information.[52] Medicare Australia also had concerns about identifying what an agency or organisation is 'likely' to do.[53] One stakeholder noted that assessments of 'likelihood' are difficult to make as they are highly contextual and require a detailed consideration of the relevant circumstances.[54]

6.39 Another stakeholder noted that, in large and disparate organisations, even where information is held by the same organisation, it may not be combined in such a way as to identify individuals.[55] BPAY stated that it was

> unreasonable, that an organisation should be required to be aware of the various technologies and information which is available, to combine all information that it has capacity to access and apply it to all personal information collected.[56]

---

49 Ibid.
50 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
51 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
52 Law Council of Australia, *Submission PR 527*, 21 December 2007.
53 Medicare Australia, *Submission PR 534*, 21 December 2007.
54 Confidential, *Submission PR 536*, 21 December 2007.
55 P Youngman, *Submission PR 394*, 7 December 2007.
56 BPay, *Submission PR 566*, 31 January 2008.

About an individual

6.40 Veda Advantage noted that if the definition of 'personal information' were expanded to include information that 'referred to' or 'related to' an individual, it would make large scale data studies—where privacy is protected by de-identifying information or encrypting significant elements—impossible.[57]

6.41 One other issue that arose in submissions and consultations was whether business or commercial information was 'about' an individual—for example, information on the number and type of prescriptions issued by a particular health service provider, where patient identifiers have been removed. It was suggested that this kind of information should not be protected by the *Privacy Act* as it relates to the health service provider's business practices, rather than his or her personal affairs.[58] The Article 29 Data Protection Working Party, however, has stated that:

> Drug prescription information … whether in the form of an individual prescription or in the form of patterns discerned from a number of prescriptions, can be considered as personal data about the physician who prescribes this drug, even if the patient is anonymous.[59]

6.42 The OPC has also stated that, if an individual's identity can be determined from business information, the information is personal information for the purposes of the *Privacy Act*.[60] The Australian Government noted in its response to the recommendations of the *Taskforce on Reducing the Regulatory Burden on Business* that the publication of detailed information on the charging practices and performance of health service providers is likely to have industry wide implications and any proposed reform would need to take these implications into account.[61]

6.43 While the *Privacy Act* would not stand in the way of this kind of regulatory reform, in the absence of such reform the *Privacy Act* will apply to such information. The extent to which business or commercial information is 'about' an individual and, therefore, constitutes 'personal information' is also considered in Chapter 54 in relation to credit reporting information and Chapter 63 in relation to health information.

Ability to contact

6.44 In its submission to the Inquiry, PIAC noted the Senate Committee privacy inquiry view that consideration should be given to extending the definition of 'personal

---

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

58 Australian Health Insurance Association, *Submission PR 161*, 31 January 2007; IMS Health Asia, *Consultation PC 124*, Sydney, 8 March 2007.

59 European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP136 (2007).

60 Office of the Privacy Commissioner, *Frequently Asked Questions: When is Business Information Covered by the Privacy Act?* <www.privacy.gov.au/faqs/bf/q8.html> at 30 April 2008.

61 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 5–6.

information' to include information 'that enables an individual not only to be identified, but also contacted'.[62] PIAC expressed support for this view on the basis that the right to be left alone is an important element of the right to privacy and should be included in the *Privacy Act*.[63]

6.45 On the other hand, Australia Post was concerned that extending the definition in this way would prevent businesses contacting individuals, even where they are not identified or identifiable, and would be inconsistent with the policy objectives of the *Privacy Act*.[64]

6.46 The OPC has made clear that a business can use personal information taken from public sources—such as the phone book—to contact potential customers. Thus, even if contact information were 'personal information', businesses could use the information to contact individuals. The obligations imposed by the *Privacy Act* in these circumstances would be to:

- tell potential customers the business' name and how to contact it, why the information has been collected, to whom the business usually discloses such information and how the customer can get access to the information (NPP 1.5);
- only use the information for the purpose it was collected, that is, to approach the customer, or for a related purpose that the potential customer would expect (NPP 2.1(a));
- do what is reasonable to make sure the information is correct and to delete or correct information that it finds is not correct (NPP 3);
- keep the information reasonably secure (NPP 4);
- have a privacy policy (NPP 5); and
- give the potential customer access to the information on request and correct any errors the customer points out (NPP 6).[65]

6.47 The Cyberspace Law and Policy Centre agreed with the ALRC that information that simply allows an individual to be contacted without conveying anything about the individual's identity or characteristics should not fall within the proposed definition of

62 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.14].
63 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
64 Australia Post, *Submission PR 78*, 10 January 2007.
65 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001).

'personal information' and suggested that this be clarified in the legislation or the Explanatory Memorandum.[66]

ALRC's view

6.48 The current definition of 'personal information' contains the following elements:

- information or an opinion;
- including information or an opinion forming part of a database;
- whether true or not;
- whether recorded in a material form or not;
- about an individual;
- whose identity is apparent from the information or opinion; or
- whose identity can reasonably be ascertained from the information or opinion.[67]

6.49 Although a number of these elements are unproblematic, the ALRC's view is that one element is unnecessary and that others do not reflect the standards set in international instruments dealing with the privacy of personal information and should be changed.

Elements requiring no change

6.50 The following elements of the definition of 'personal information' should remain unchanged: information or an opinion; whether true or not; and whether recorded in a material form or not. The ALRC received very few submissions indicating that these elements of the definition were problematic.

6.51 Personal information should be 'about' an individual. The ALRC notes that, although a number of international instruments use the term 'relates to', the *Privacy Act* terminology is consistent with the APEC Privacy Framework and reflects that fact that the information must be about an identified or reasonably identifiable individual.

---

66 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
67 *Privacy Act 1988* (Cth) s 6(1).

Forming part of a database

6.52 The second element of the definition—'including information or an opinion forming part of a database'—is unnecessary and should be deleted. It may have been helpful to make this clear in 1988 when the *Privacy Act* was originally passed, but in the current environment it is no longer a matter of uncertainty. In addition, the recommended definition of 'record', discussed below, expressly includes 'information stored in electronic or other formats'.[68]

Whose identity is apparent or can reasonably be ascertained from the information

6.53 This element of the definition should be amended to bring it more into line with other jurisdictions and international instruments. Noting the distinction between 'identity' and 'identification', discussed above, the *Privacy Act* should apply to information about an individual who is 'identified or reasonably identifiable' rather than information about an individual whose 'identity' is apparent, or reasonably ascertainable. The APEC Privacy Framework, the OECD Guidelines, the Council of Europe Convention and the EU Directive use the terms 'identified' and 'identifiable'. The recommended terminology is more consistent with this language and international jurisprudence and explanatory material based on the terms 'identified' and 'identifiable' will be more directly relevant.

6.54 The definition of personal information should include an element of reasonableness. Whether an individual can be identified or is identifiable depends on context and circumstances. While it may be technically possible for an agency or organisation to identify individuals from information it holds, for example, by linking the information with information held by another agency or related organisation, it may be that it is not practically possible. For example, logistics or legislation may prevent such linkage. In these circumstances, individuals are not 'reasonably identifiable'.

6.55 In addition, the definition of 'personal information' should not be limited, as it currently is, to information about an individual whose identity is apparent or can reasonably be ascertained 'from the information'. An individual is 'reasonably identifiable', when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation may access without unreasonable cost or difficulty.

6.56 The ALRC notes the concerns raised by stakeholders, particularly about the proposed clarification to be included in the Explanatory Memorandum—that information is reasonably identifiable when an individual can be identified from information in the possession of an agency or organisation or from that information

68 Rec 6–6.

and other information the agency or organisation has the capacity to access or is likely to access. While this test is included expressly in the *Data Protection Act 1998* (UK), it may lack sufficient flexibility and should not be included in the amended *Privacy Act* or Explanatory Memorandum.

6.57 As noted by Microsoft Asia Pacific, whether an individual is 'reasonably identifiable' from certain information requires a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such as way as to identify him or her. This is an appropriate formulation of the test. The ALRC does not agree with the Australian Privacy Foundation that the test should be whether an individual is 'potentially identifiable'. A great deal of information is about potentially identifiable individuals but where identifying the individuals would involve unreasonable expense or difficulty, and is unlikely to happen, the ALRC is of the view that the information is not 'personal information' for the purposes of the *Privacy Act*.

6.58 As noted by the OPC, the issue is also context specific. Information that is not 'personal information' in a particular context is discussed further below in relation to research. Where an independent intermediary, such as the Western Australian Data Linkage Unit (DLU), is used to remove identifying particulars and to code information provided to researchers the information in the hands of the researchers is not about 'identified or reasonably identifiable' individuals for the purposes of the *Privacy Act*. The individuals remain, however, 'potentially identifiable'.

6.59 The ALRC notes the United Kingdom Information Commission's view that information need not be linked to a name and address in order for the individual to be 'identified'. The examples provided include: the collection of information about internet users with the intention of linking that information to names and addresses; and targeting individuals with advertising without linking the information to names and addresses or making any effort to identify individuals in the physical world. The Information Commissioner takes the view that such information is 'personal data'. This information would also fall within the recommended definition of personal information and should be protected by the *Privacy Act*.

6.60 While stand alone telephone numbers, street addresses and IP addresses may not be personal information for the purposes of the *Privacy Act*, such information may become personal information in certain circumstances. The ALRC acknowledges that telephone numbers relate to telephones or other communications devices, IP addresses to computers, and street addresses to houses, rather than individuals, but notes that such information may come to be associated with a particular individual as information accretes around the number or address. The ALRC notes ACMA's concern that it may be difficult to determine when an IP address becomes personal information. It is the ALRC's view, however, that given the exceptions provided in the model UPPs for actions required or authorised by or under law, investigations of suspected unlawful activity and for enforcement activities, this issue will not hinder investigative and enforcement action by the Authority.

Ability to contact

6.61 Information that simply allows an individual to be contacted—such as a telephone number, a street address or an IP address in isolation—would not fall within the recommended definition of 'personal information'. As noted above, the *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. As information accretes around a point of contact and it becomes possible to link that information to a particular individual and to target that individual—for example, with advertising material—the information becomes 'personal information' for the purposes of the Act. If an agency or organisation can reasonably identify direct mail recipients by linking data in an address database with particular names in the same or another database, that information is 'personal information' and should be treated as such.

Conclusion

6.62 The then Privacy Commissioner, Malcolm Crompton, expressed the view that:

> Privacy laws need to be in the form of general principles, as information handling is highly contextual. This can create a significant margin for interpretation and implementation.[69]

6.63 Because of this, elements of the definition of 'personal information' will continue to give rise to theoretical uncertainty. While much information will fall clearly inside or outside the definition, there will be a need for ongoing practical guidance in relation to areas of uncertainty. The OPC has suggested that it issue further guidance on the meaning of 'personal information'. The ALRC agrees that such guidance will be necessary to indicate how the definition operates in specific contexts. In particular, the ALRC recommends that the OPC develop and publish guidance on the meaning of 'identified or reasonably identifiable'.

Recommendation 6–1 The *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

Recommendation 6–2 The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'identified or reasonably identifiable'.

69 M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002).

What is not 'personal information'?

6.64 As well as considering what information falls within the definition of 'personal information' for the purposes of the *Privacy Act*, it is also important to consider what information would fall outside the definition on the basis that it is not 'about an individual whose identity is apparent or can reasonably be ascertained'.[70] The OPC Review identified a number of problems in this area. Stakeholders, particularly those involved in research, stated that it was difficult to determine when information was 'de-identified' for the purposes of the *Privacy Act*.[71] In response, the OPC Review stated that:

> As part of a wider inquiry into the *Privacy Act*, the issue of what is or is not de-identification could be considered. This is an important threshold issue which determines whether or not information is protected. Developments in technology have made it increasingly difficult to determine whether information is de-identified or not. In the meantime, the Office could provide guidance on this, which would help HRECs [Human Research Ethics Committees] and researchers in their decision making.[72]

6.65 There is a strong public interest in the collection, use and disclosure of personal information that has been 'de-identified' for activities such as research. That is not to suggest that individuals have no interest in such information about them, but that the individual's interest in the information may at some point give way to the broader public interest in being able to use the information freely.

6.66 The EU Directive makes clear that the privacy principles do not apply to information that has been 'rendered anonymous' so that individuals are no longer identifiable. The Directive suggests that codes of conduct may be necessary to provide guidance on ways in which information can be 'rendered anonymous' and retained in a form in which identification is no longer possible.[73]

6.67 The National Health and Medical Research Council (NHMRC), the Australian Research Council and the Australian Vice Chancellors Committee also considered this issue in the context of producing the revised *National Statement on Ethical Conduct in*

---

70 In Ch 28 the ALRC considers what steps are necessary to meet the requirement in the 'Data Security' principle to take reasonable steps 'to destroy or render non-identifiable personal information when it is no longer needed for any purpose for which it can be used or disclosed under the UPPs; and retention is not required or authorised by or under law'. The ALRC recommends that the Privacy Commissioner develop and publish guidance on these issues including the manner in which information should be destroyed or rendered non-identifiable: Rec 28–5.

71 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.

72 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.

73 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 26.

Human Research (the National Statement).[74] The National Statement makes a distinction between individually identifiable data, re-identifiable data and non-identifiable data as follows:

> Data may be collected, stored or disclosed in three mutually exclusive forms:
>
> - individually identifiable data, where the identity of a specific individual can reasonably be ascertained. Examples of identifiers include the individual's name, image, date of birth or address;
> - re-identifiable data, from which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets;
> - non-identifiable data, which have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. A subset of non-identifiable data are those that can be linked with other data so it can be known that they are about the same data subject, although the person's identity remains unknown.
>
> This National Statement avoids the term 'de-identified data', as its meaning is unclear. While it is sometimes used to refer to a record that cannot be linked to an individual ('non-identifiable'), it is also used to refer to a record in which identifying information has been removed but the means still exist to re-identify the individual. When the term 'de identified data' is used, researchers and those reviewing research need to establish precisely which of these possible meanings is intended.[75]

Issues Paper questions

6.68 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act*, like the National Statement, should include definitions of terms such as 're-identifiable' and 'non-identifiable' and whether a distinction should be drawn between identifiable personal information and re-identifiable personal information.[76]

6.69 In response, the Western Australian Department of Health suggested that, in the context of the *Privacy Act*, there are only two relevant categories of personal information:

- reasonably identifiable personal information; and
- non-identifiable information.[77]

---

74 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007). The National Statement is discussed in detail in Chs 64 and 65.

75 Ibid, 29.

76 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 8–27 and 8–28.

77 Department of Health Western Australia, *Submission PR 139*, 23 January 2006.

6.70 The Department's view was that 'reasonably identifiable personal information' includes information linked with an individual's name, image, date of birth or address; information that contains a unique personal identifier when the holder of the information also has the master list linking the identifiers to individuals; information that the holder can merge or link to other information they already hold, enabling them to identify individuals; and aggregated information where individuals can be identified because of the small number of individuals in particular fields of information.

6.71 The Department stated that 'non-identifiable information' includes information that has never been labelled with individual identifiers or from which they have been permanently removed; and information that contains a unique personal identifier where the holder cannot link the information to a specific individual because they do not hold the master list linking the identifiers to individuals.[78]

6.72 The Department also made the point that identifiability is contextual: information that is identifiable to the original holder of the information may be non-identifiable to a recipient of the information. For example, information that contains a unique personal identifier is not identifiable to a recipient who does not hold the master list. This is the basis of the data linkage protocol adopted by the DLU in Western Australia, discussed further in Chapter 66. Other stakeholders agreed that the use of independent intermediaries means that the information in the hands of data recipients should not be classified as 're-identifiable' but, for the purposes of the *Privacy Act*, should be considered 'non-identifiable'.[79]

6.73 The Australian Government Department of Health and Ageing (DOHA) noted the need for guidance on the meaning of terms such as 'identified', 're-identifiable', 'non-identifiable' and 'de-identified' but did not believe the terms needed to be defined in the *Privacy Act*.[80] Other stakeholders felt that definitions would be helpful, with some noting the importance of maintaining consistency with the National Statement.[81]

6.74 Some stakeholders expressed the view that no distinction should be drawn between 'identifiable' and 're-identifiable' personal information in the context of the *Privacy Act*.[82] The Australian Privacy Foundation stated that:

---

78 Ibid.

79 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006.

80 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

81 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Queensland Institute of Medical Research, *Submission PR 80*, 11 January 2006; A Smith, *Submission PR 79*, 2 January 2007 Caroline Chisholm Centre for Health Ethics, *Submission PR 69*, 24 December 2006.

82 Australian Nursing Federation, *Submission PR 205*, 22 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

> Health researchers have constructed elaborate mechanisms to allow data linkage, which provide a degree of protection but do not amount to de-identification. Information either is or is not actually or potentially identifiable. The ALRC should be wary about legitimizing the idea that there can be an intermediate category.[83]

Discussion Paper proposal

6.75 In DP 72, the ALRC agreed with the position put by the Western Australian Department of Health, and expressed the view that it is unnecessary to include definitions of the terms 're-identifiable' and 'non-identifiable' in the *Privacy Act*. The relevant categories of information, for the purposes of the Act, are information that is about an 'identified' individual and information about a 'reasonably identifiable' individual. All other information falls outside the definition of personal information and is not covered by the Act. The ALRC proposed that the Privacy Commissioner issue guidance on the meaning of 'not reasonably identifiable'.[84]

Submissions and consultations

6.76 In response to DP 72, the Australian Privacy Foundation expressed the view that, even if 'significant effort is required' to identify individuals from information or a dataset, the data is 'reasonably identifiable'. The Foundation noted that many agencies and organisations have the resources to make such 'significant efforts'. In addition, advances in technology mean that re-identifying individuals is becoming easier. The Foundation suggested that the guidance to be issued by the Privacy Commissioner should recommend that information be rendered non-identifiable wherever possible, and ensure that the practical and technological implications of changes in this area are assessed fully.[85]

6.77 Medicare Australia noted that it categorised personal information as 'statistical', 'identified', and 'identifiable', and that the agency has developed internal guidelines to assist with decisions regarding release of information as follows:

- statistical information—there is no reasonable likelihood that the person who receives the information could identify any individuals, through analysis of the information either by itself or in association with other information available to the user;
- identified information—includes any unique or specific identifiers, such as names, addresses, or case numbers that can be linked to other identifiers by the user; and

83 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.
84 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 58–10.
85 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

- identifiable information—does not include identifiers but analysis of the information either by itself or when linked to other information available to the user might lead to the identification of individuals.[86]

6.78 The Australian Government Department of Human Services explained that, in deciding whether to disclose de-identified personal information to researchers, Medicare Australia carefully considered what was released in order to ensure that individuals could not be identified or re-identified. This consideration included examining what other information researchers were collecting and considering whether that information could be linked with information released by Medicare Australia in a way that would enable researchers to identify individuals.[87] A number of other stakeholders also suggested that it was necessary to consider each disclosure on a case-by-case basis to avoid releasing information that might identify an individual, for example, because of the small number of individuals in the data set.[88]

6.79 The Australian Bureau of Statistics (ABS) and other agencies employ a range of techniques to minimise the risk of disclosing information that might be used to identify individuals. These include data suppression, data rounding and category collapsing. Detailed categories such as country of birth or industry or occupation can be collapsed to a less detailed level to avoid the risk of identification. Such techniques, however, can have a negative impact on the usefulness of data as some detailed data may need to be suppressed or modified.[89] The *National Statistical Service Handbook* provides guidance on these matters for Australian and state and territory government agencies.[90]

6.80 The CSIRO referred in its submission to the extremely detailed guidance provided in s 164 of the *Health Insurance Portability and Accountability Act 1996* (US) (HIPA Act), which provides a number of tests to determine when information is not 'individually identifiable health information'. The first test allows 'a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable' to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information.[91]

6.81 An alternative test in the legislation expressly sets out a long list of identifiers that must be removed to render the information not individually identifiable. The list

---

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

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

88 Australian Bureau of Statistics, *Consultation PC 139*, Canberra, 16 March 2007; B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; National E-Health Transition Authority, *Consultation PC 41*, Sydney, 6 December 2006.

89 National Statistical Service, *National Statistical Service Handbook* <www.nss.gov.au/nss/home.NSF/pages/NSS+Resources?OpenDocument> at 30 April 2008.

90 Ibid, App 4 Confidentiality and Privacy.

91 *Health Insurance Portability and Accountability Act of 1996* Pub L 104–191, 110 Stat 1936 (US) s 164.514(b)(1). CSIRO, *Submission PR 176*, 6 February 2007.

includes: names; all geographic subdivisions smaller than a State; all elements of dates related to an individual apart from year; telephone and fax numbers; electronic mail addresses; social security numbers; medical record numbers; web Universal Resource Locators; IP address numbers; and so on. In addition, the relevant entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual.[92]

6.82 In response to the ALRC's proposal that the Privacy Commissioner should issue guidance on the meaning of 'not reasonably identifiable', the Victorian Health Services Commissioner stated that such guidance will be necessary because the issue is contextual and must be decided on a case-by-case basis.[93] A number of other stakeholders, including the OPC, agreed.[94]

ALRC's view

6.83 In the ALRC's view, it is unnecessary to include definitions of 're-identifiable data' and 'non-identifiable data' in the *Privacy Act.* For the purposes of the Act it is necessary to decide 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. This includes making a distinction between information that may be 're-identifiable' or reasonably identifiable in a particular context—for example, where an agency or organisation holds information identified by a unique identifier and also holds the master list—but is not reasonably identifiable for the purposes of the Act in another context—for example, where an agency or organisation holds information identified by a unique identifier but does not hold and does not have access to the master list.

6.84 The ALRC notes that this last category of information falls into the National Statement's 'non-identifiable' category. For the purposes of the *Privacy Act*, however, it is sufficient to regard the information as 'not reasonably identifiable'. If the risk of identification from particular information in a particular context is very small, a decision will have to be taken as to whether, on objective grounds, the information is 'reasonably identifiable'.

---

92 *Health Insurance Portability and Accountability Act of 1996* Pub L 104–191, 110 Stat 1936 (US) s 164.514(b)(2).

93 Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007.

94 Government of South Australia, *Submission PR 565*, 29 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Prescribing Service, *Submission PR 547*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; University of Newcastle, *Submission PR 413*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

6.85 Guidance provided by the Privacy Commissioner would be of great value to those making decisions on a case-by-case basis on these matters. Such guidance might refer to or include guidance of the sort provided in the National Statistical Service Handbook[95] or the provisions of the HIPA Act discussed above. Developing and publishing guidance, rather than making legislative rules, allows a more flexible and nuanced response to particular situations.

6.86 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96),[96] the ALRC and the Australian Health Ethics Committee (AHEC) of the NHMRC considered the use of independent intermediaries to hold codes linking genetic samples or information with identifiers. The ALRC and AHEC concluded that use of an independent intermediary (such as a 'gene trustee') is an effective method of protecting the privacy of samples and information held in human genetic research databases. The system maintains the privacy of samples and information, while allowing donors to be contacted if necessary. It ensures that anyone who obtains access to samples and information is unable to re-identify them without the authorisation of the gene trustee.[97]

6.87 This kind of arrangement might also provide appropriate protection in relation to other personal information, but this will depend on the arrangements established between data custodians, intermediaries and data recipients. If appropriate arrangements are put in place, such that data recipients are not able to identify individuals, the information held by the data recipient is likely to be not reasonably identifiable in that context and no longer 'personal information' for the purposes of the *Privacy Act.*

Recommendation 6–3 The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'not reasonably identifiable'.

Sensitive information

6.88 'Sensitive information' is a sub-set of personal information and is given a higher level of protection under the NPPs. The IPPs do not refer to sensitive information and agencies are required to handle all information, including sensitive information, in accordance with the IPPs. The principles recommended for handling sensitive information, and their extension to agencies, are discussed further in Chapter 22.

95 National Statistical Service, *National Statistical Service Handbook* <www.nss.gov.au/nss/home.NSF/pages/NSS+Resources?OpenDocument> at 30 April 2008.

96 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

97 Ibid, [18.102]–[18.117].

6.89 'Sensitive information' is defined in the *Privacy Act* to mean information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices; or
- criminal record.

6.90 'Sensitive information' also includes health information[98] and genetic information about an individual that is not otherwise health information.[99]

6.91 'Sensitive information' is subject to a higher level of privacy protection than other 'personal information' handled by organisations in the following ways:

- 'sensitive information' may only be collected with consent, except in specified circumstances. Consent is generally not required to collect 'personal information' that is not 'sensitive information';[100]

98 *Privacy Act 1988* (Cth) s 6(1). The definition of 'health information' is discussed in Ch 62.

99 *Privacy Legislation Amendment Act 2006* (Cth). In the report *Essentially Yours* (ALRC 96), the ALRC and AHEC considered the definition of 'sensitive information'. They came to the conclusion that the definition did not provide an appropriate level of protection for genetic information that did not fall within the definition of health information—for example, genetic information derived from parentage or other identification testing that is not predictive of health—and recommended that the definition be amended to clarify this issue: Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–5. The Australian Government accepted this recommendation and the relevant amendment came into force in September 2006.

100 *Privacy Act 1988* (Cth) sch 3, NPP 10.

- 'sensitive information' must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual;[101]

- 'sensitive information' cannot be used for the secondary purpose of direct marketing;[102] and

- 'sensitive information' cannot be shared by 'related bodies corporate' in the same way that they may share other 'personal information'.[103]

6.92 Similar classes of personal information are included in the definitions of 'sensitive information' in the Victorian, Tasmanian and Northern Territory privacy legislation.[104] Health information is not included in the definition of 'sensitive information' in Victoria because it is covered separately by the *Health Records Act 2001* (Vic). The *Privacy and Personal Information Protection Act 1998* (NSW) does not include a definition of sensitive information.

6.93 The Council of Europe Convention and OECD Guidelines do not specifically address sensitive information. Indeed, the Explanatory Memorandum to the OECD Guidelines expresses the view that 'it is probably not possible to identify a set of data which are universally regarded as being sensitive'.[105]

6.94 Article 8 of the EU Directive deals with 'special categories of data', which are defined as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. Article 8 prohibits the processing of this kind of information without consent except in specified circumstances and allows Member States to prohibit processing such data even with the consent of the data subject. The EU Directive also refers to 'sensitive data' but does not define the term.[106]

6.95 Sensitive information is provided with additional protection in the *Privacy Act* for a number of reasons. Information relating to race or ethnic origin, political or religious beliefs, trade union membership and sexual orientation, for example, is highly personal and may provide the basis for unjustified discrimination. In addition, this sort of information is likely to be necessary for the functions and activities of agencies and organisations in very limited circumstances. Health information, genetic information

---

101 Ibid sch 3, NPP 2.1(a).
102 Ibid sch 3, NPP 2.1(c).
103 Ibid s 13B.
104 *Information Privacy Act 2000* (Vic) sch 1; *Personal Information Protection Act 2004* (Tas) s 3; *Information Act 2002* (NT) s 4. Note, however, that the Northern Territory Act does not specifically refer to 'an opinion' about those matters.
105 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19].
106 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 34, 70.

and criminal record information also is highly personal and has the potential to give rise to unjustified discrimination against individuals.

6.96 In IP 31, the ALRC asked whether the existing definition of 'sensitive information' was adequate and appropriate.[107] The major issues raised by stakeholders in response were: information made sensitive by context; financial information; and biometric information.

Information made sensitive by context

6.97 In its submission to the Inquiry, the NHMRC stated that:

> it is extremely difficult to establish the categories of information which universally would be considered 'sensitive' either because of the nature of the information, the context in which it is handled or the views of the person to whom the information relates.
>
> We note that the *Personal Information Protection and Electronic Documents Act 2000* (Canada) does not define 'sensitive information' and that the Model Code allows an organisation discretion in determining whether information is sensitive. We also note that the sensitivity of certain categories of information may vary between cultures and individuals.[108]

6.98 The Canadian *Personal Information Protection and Electronic Documents Act 2000* states that:

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.[109]

6.99 The NHMRC suggested that the categories of information included in the definition of 'sensitive information' might be amended by regulation to provide some flexibility.[110] The CSIRO suggested that sensitive information should include 'culturally sensitive data' or other data deemed to be sensitive by the data provider.[111]

---

107 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 3–4.
108 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
109 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, cl 4.3.
110 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
111 CSIRO, *Submission PR 176*, 6 February 2007.

6.100 The Queensland Government Commission for Children and Young People and Child Guardian noted that:

> For instance, a health practitioner receiving information relating to the abuse or neglect of a child may consider this information to be health information, and hence deal with it under the specific health privacy regime. However, if the same information is received by a child welfare practitioner it is not likely to be considered purely health information. The classification of child abuse information thus appears to depend not only on its nature, but also the context in which it is received.[112]

6.101 DLA Phillips Fox, however, suggested that:

> Introducing more subjective criteria (such as the sensitivity of the information taking into account surrounding circumstances) would:
>
> - result in greater uncertainty of application; and
> - reduce the ability of organisations to implement broad guidelines for the treatment of categories of information so as to ensure compliance with the NPPs (and equivalent state and territory requirements).[113]

ALRC's view

6.102 The ALRC recognises that personal information can become more or less sensitive because of the context in which it is considered and notes that this can apply to almost any personal information. The definition of 'sensitive information', however, should not be amended to include information made sensitive by context. On balance, the existing approach of listing categories of information as sensitive provides greater certainty. This is important because the *Privacy Act* imposes stringent requirements for handling sensitive information.

6.103 In particular, the *Privacy Act* and the model UPPs provide that sensitive information should generally be collected with consent and should be used only for the purpose for which the information was collected or a directly related secondary purpose. This regime is significantly different to the regime regulating the handling of other personal information, which can be collected without consent and used and disclosed for a broader range of purposes. It is important to be clear about what information is covered by the more stringent requirements.

---

112 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

113 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

Financial information

6.104 A number of stakeholders suggested that sensitive information should include financial information,[114] while others described consumer credit information as sensitive.[115] The OPC stated that:

> Community attitudes research undertaken by the Office in 2001 and 2004 has indicated that individuals consider financial information to be very sensitive. In both community attitudes surveys, financial information was the top response for individuals when rating what types of information they were most reluctant to provide to organisations.[116]

6.105 Legal Aid Queensland, however, noted in its submission:

> That obtaining consent as the primary criteria for the release of financial information fails to recognise the inherent disparity in the bargaining positions of consumers and corporations.[117]

6.106 A number of other stakeholders were of the view that financial information should not be included in the definition of 'sensitive information'.[118]

ALRC's view

6.107 Financial information should not be included in the definition of 'sensitive information' in the *Privacy Act*. Financial information is sensitive in some respects and does require appropriate handling, for example, appropriate security. Financial information has a number of characteristics, however, that sets it apart from the categories of information currently included in the definition of sensitive information. In particular, it does not relate to the physical attributes or personal beliefs of the individual in the same way as other information currently defined as sensitive.

6.108 In addition, agencies and organisations often have a legitimate interest in an individual's financial information, for example, in relation to providing credit. Such information is necessary to the functions and activities of agencies and organisations in order to protect the interests of all parties to transactions. The *Privacy Act* already recognises that personal information relating to credit can be prejudicial and should only be collected, used and disclosed in appropriate circumstances. The Act provides a

---

114 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

115 National Legal Aid, *Submission PR 265*, 23 March 2007; J Harvey, *Submission PR 12*, 25 May 2006.

116 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See Office of the Privacy Commissioner, Community Attitudes Research 2001, 2004, available at <www.privacy.gov.au/business/research/index.html>.

117 Legal Aid Queensland, *Submission PR 292*, 11 May 2007.

118 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

range of safeguards in relation to credit reporting that are discussed in detail in Part G. It is important to note, however, that these safeguards are not the same as the safeguards provided in relation to 'sensitive information'. For example, the credit reporting provisions do not require consent for the collection of credit information.

Biometric information

6.109 Biometric information can be 'personal information' for the purposes of the *Privacy Act* in some circumstances, that is, where an individual's identity is apparent or can reasonably be ascertained from the information.[119] A number of stakeholders suggested that biometric information, like genetic information, should be accorded the higher protection provided by the *Privacy Act* in relation to 'sensitive information'.[120] Concern has been expressed that biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent,[121] and that biometric information could reveal other sensitive personal information, such as information about a person's health, racial or ethnic origin or religious beliefs.[122]

6.110 The Biometrics Institute describes the nature of biometric technology as follows:

> Biometric technology involves the storage and use of unique personal information to verify the identity of an individual. These unique identifiers are based on personal attributes such as fingerprints, DNA, iris, facial features, hand geometry, voice etc. Even a photograph could be described as one of the lower levels of biometric recognition.[123]

6.111 As discussed in Chapter 9, in a typical biometric system a biometric device, such as a finger scanner, is used to take a biometric sample from an individual. Data from the sample are then analysed and converted into a biometric template, which is stored in a database or an object in the individual's possession, such as a smart card. Later biometric samples taken from the individual can then be compared to the stored biometric template to identify the individual (identification, or one-to-many matching) or to attempt to verify that an individual is who he or she claims to be (verification, or one-to-one matching).

---

119 Biometric systems technologies are discussed further in Ch 9.

120 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; AAMI, *Submission PR 147*, 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

121 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12–13.

122 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), 6; M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

123 Biometrics Institute, *Biometrics Institute Privacy Code Information Memorandum* (2006), 1.

6.112 Recognising some of the special sensitivities around the use of biometric technology, the Biometrics Institute, in consultation with the OPC, has developed a privacy code to regulate the handling of biometric information.[124] The code binds private sector organisations that apply to become Code Subscribers and whose applications are approved by the Biometrics Institute Board. To date, only four organisations have elected to be bound by the Code.

6.113 The *Biometrics Institute Privacy Code* includes a number of Supplementary Biometrics Institute Privacy Principles. One of the additional principles is similar in scope to the protection provided for 'sensitive information' by NPP 2.1(a):

> Secondary analysis or function creep of biometric information collected for purposes such as authentication or identification is not permitted without express free and informed consent. For example biometric information collected for the purposes of authentication and identification shall not be used to examine that information in search of genetic patterns or disease identification without express free and informed consent.[125]

6.114 In its submission to the Inquiry, the Health Informatics Society of Australia noted that:

> Sensitive information by definition relates to those areas where prejudices can prevail, eg sexual preferences, political or religious beliefs, criminal records, etc. The concern individuals have over the way that other parties might act based on the knowledge gained from genetic information puts this into the sensitive information category. Furthermore, biometric information can be considered sensitive since it is fixed and unlike a password or PIN cannot be reset once it has been inappropriately released.[126]

6.115 The OPC expressed the view that

> all biometric template information should be covered by the stricter provisions in the *Privacy Act* for sensitive information. However, it may be impractical and undesirable for all biometric samples to be included under the definition of sensitive information, especially where there is no intention to use the sample for biometric matching or identification. For example, it would be difficult and overly burdensome to require consent every time a photograph of a person (technically a biometric sample) is taken.
>
> The Office takes the view that sensitive information provisions should only apply to: (a) biometric samples collected for the purpose of biometric matching or biometric identification; and (b) biometric template information.
>
> The Office notes however that biometric samples—if they were to fall outside this definition of sensitive information—may still be covered by the *Privacy Act* as personal information and therefore achieve legislative protections. Furthermore, as noted in IP31 (at IP31 paragraph 11.46) there may be instances where a biometric

---

124 Biometrics Institute, *Biometrics Institute Privacy Code* (2006).
125 Ibid, 12.3.
126 Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007.

> sample reveals sensitive information about an individual such as health information and will thus be defined as sensitive information under the *Privacy Act*.[127]

Discussion Paper proposal

6.116 In DP 72 the ALRC proposed that the definition of 'sensitive information' be amended to include: biometric information collected for the purpose of automated biometric authentication or identification; and biometric template information.[128] There was significant support for this proposal.[129]

6.117 A small number of stakeholders did not support the proposal.[130] The Australian Government Department of Defence did not support extending the definition of 'sensitive information' to include biometric template information.[131]

6.118 Professor Michael Wagner, of the National Centre for Biometric Studies at the University of Canberra, noted in correspondence to this Inquiry that biometric templates contain 'all the salient information necessary to authenticate or identify a person' and that 'this will potentially include sensitive information related to age, gender, [and] health'. He stated that:

> Biometric templates are not *essentially* different from the original biometric information. Therefore I believe that *both* original biometric information *and* biometric templates should equally be treated as sensitive and protected correspondingly.[132]

ALRC's view

6.119 The definition of sensitive information should be amended to include certain biometric information. Biometric information shares many of the attributes of information currently defined as sensitive in the *Privacy Act*. It is very personal because it is information about an individual's physical self. Biometric information can reveal other sensitive information, such as health or genetic information and racial or ethnic origin. Biometric information can provide the basis for unjustified discrimination.

---

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

128 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–6.

129 Unisys, *Submission PR 569*, 12 February 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 Government Department of Human Services, *Submission PR 541*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 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; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Law Society of New South Wales, *Submission PR 443*, 10 December 2007; 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.

130 Confidential, *Submission PR 536*, 21 December 2007.

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

132 M Wagner, *Correspondence*, 16 January 2008.

6.120 The ALRC recognises that requiring consent to collect all biometric information may be impracticable. For this reason, the ALRC has limited the type of biometric information to be included in the definition of sensitive information—namely, biometric information collected for use in automated biometric verification and identification systems and biometric template information. This recommendation is intended to address the most serious privacy concerns around the handling of biometric information, for example, that such information may be used to identify individuals without their knowledge or consent.

6.121 The provisions of the *Privacy Act* relating to sensitive information do not currently apply to agencies. In Chapter 22, the ALRC recommends that the requirements in the model UPPs dealing with 'sensitive information' apply to both agencies and organisations.[133] The ALRC also recommends broadening the circumstances in which sensitive information may be collected without consent to include collection 'required or authorised by or under law' to meet concerns raised by agencies.[134] Where biometric information is to be collected by agencies, for example, for inclusion in automated biometric verification or identification systems, such as the 'SmartGate' automated border processing system,[135] such collection should be carried out on the basis of consent, or as required or authorised by or under law.

Sexual orientation and practices

6.122 In DP 72, the ALRC also suggested that the reference to 'sexual preferences and practices' in the definition of 'sensitive information' be changed to 'sexual orientation and practices'.[136] This was on the basis that the term 'sexual orientation' is consistent with language used in recent federal legislation[137] and state and territory anti-discrimination and human rights legislation.[138] It also reflects modern usage. A number of stakeholders expressed support for this change.[139]

---

133 Rec 22–1.

134 Rec 22–2.

135 SmartGate is an automated border processing system. It performs the customs and immigration checks normally made by a Customs Officer on arrival in Australia. SmartGate takes a live image of an individual's face and using facial recognition technology matches that image with the digitised image stored in an ePassport.

136 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–7.

137 *Private Health Insurance Act 2007* (Cth) s 55.5.

138 *Equal Opportunity Act 1995* (Vic) s 6; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 3; *Equal Opportunity Act 1984* (WA) s 35O; *Anti-Discrimination Act* 1998 (Tas) s 16; *Human Rights Act 2004* (ACT) s 8.

139 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 Government Department of Human Services, *Submission PR 541*, 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; Law Society of New South Wales, *Submission PR 443*, 10 December 2007.

Recommendation 6–4 The definition of 'sensitive information' in the *Privacy Act* should be amended to include:

(a) biometric information collected for the purpose of automated biometric verification or identification; and

(b) biometric template information.

Recommendation 6–5 The definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual preferences and practices'.

Records

6.123 Generally, the privacy principles in the *Privacy Act* only apply to personal information that is held, or collected for inclusion, in a 'record'.[140] The IPPs expressly refer to collection of personal information by agencies for inclusion in a 'record', storage and security of 'records', access to 'records' and so on. Section 16B provides that the Act applies to the collection of personal information by an organisation only if the information is collected for inclusion in a record or is held by the organisation in a record.

6.124 A number of the privacy Acts in other jurisdications, for example the *Privacy and Personal Information Protection Act 1998* (NSW), are not expressly limited in this way. However, in *Vice-Chancellor Macquarie University v FM*, Spiegelman CJ—with whom the other members of the New South Wales Court of Appeal agreed—found that the New South Wales Act could only sensibly apply to information held in, or collected for inclusion in, a record:

> Of particular significance is the body of consecutive sections between s 12 and s 19 of the [Privacy and Personal Information Protection] Act which adopt as their criterion of operation a reference to where a public sector agency 'holds personal information' … It is almost impossible to conceive how almost all of those other sections could operate in practice if they were intended to apply to information in the minds of employees acquired by direct visual or aural experience and never recorded in any manner.[141]

6.125 A record is defined in s 6(1) of the *Privacy Act* as follows:

(a) a document; or

(b) a database (however kept); or

---

140 The privacy principles also apply to the collection of information for inclusion in a 'generally available publication'. The definition of 'generally available publication' is discussed further below.

141 *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192, [28].

(c) a photograph or other pictorial representation of a person;

but does not include:

(d) a generally available publication; or

(e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(f) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or

(fa) records (as defined in the *Archives Act 1983*) in the custody of the Archives (as defined in that Act) in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or

(g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*; or

(h) letters or other articles in the course of transmission by post.

6.126 This section of the Report deals only with the first part of the definition, describing what is included in the definition of record. There were very few concerns raised about the second part of the definition, describing what is excluded from the definition of record, apart from one issue raised by the OPC about the definition of 'generally available publication'. This issue is considered in the following section.

6.127 The first part of the definition—which defines a record as a document, a database (however kept), or a photograph or other pictorial representation of a person—covers a broad range of recorded information including electronic records about individuals and includes photos or videos, where the person can be identified from the context or in other ways. A person's name appearing on a list of clients or patients may also fall within the definition of personal information because the context provides information about the individual.

6.128 The OPC commented that 'used in conjunction with definitions in the *Acts Interpretation Act 1901*, the definition for record is adequately broad to take in new or evolving information storage media'.[142] Section 25 of the *Acts Interpretation Act* provides:

In any Act, unless the contrary intention appears:

document includes:

(a) any paper or other material on which there is writing;

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

> (b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
>
> (c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.
>
> **record** includes information stored or recorded by means of a computer.
>
> **writing** includes any mode of representing or reproducing words, figures, drawings or symbols in a visible form.

6.129 Section 4 of the *Freedom of Information Act 1982* (Cth) (the FOI Act) sets out the following inclusive definition of document:

> (a) any of, or any part of any of, the following things:
>
> (i) any paper or other material on which there is writing;
>
> (ii) a map, plan, drawing or photograph;
>
> (iii) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them;
>
> (iv) any article or material from which sounds, images orwritings are capable of being reproduced with or without the aid of any other article or device;
>
> (v) any article on which information has been stored or recorded, either mechanically or electronically;
>
> (vi) any other record of information; or
>
> (b) any copy, reproduction or duplicate of such a thing; or
>
> (c) any part of such a copy, reproduction or duplicate;

6.130 Section 3 of the *Archives Act 1983* (Cth) defines 'record' as follows:

> **record** means a document (including any written or printed material) or object (including a sound recording, coded storage device, magnetic tape or disc, microform, photograph, film, map, plan or model or a painting or other pictorial or graphic work) that is, or has been, kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event, person, circumstance or thing.

6.131 As noted above, the *Privacy and Personal Information Act 1998* (NSW) covers information 'whether or not recorded in a material form'.[143] The Victorian and Tasmanian Acts include the requirement for information to be recorded in the definition of 'personal information'. Personal information is defined as 'information or an opinion … that is recorded in any form'[144] and 'any information or opinion in any recorded format'.[145]

---

143 *Privacy and Personal Information Protection Act 1998* (NSW) s 4.
144 *Information Privacy Act 2000* (Vic) s 3.
145 *Personal Information Protection Act 2004* (Tas) s 3.

6.132 The Western Australian Information Privacy Bill provides an inclusive definition of 'record' that sets out essentially the same elements as the *Acts Interpretation Act* definition of 'document', plus the following additional elements:

- any map, plan, diagram or graph;
- any drawing, pictorial or graphic work, or photograph; or
- any article on which information has been stored or recorded, either mechanically, magnetically or electronically.[146]

6.133 It has been noted that the requirement that personal information be held or collected for inclusion in a record means that some potentially privacy-invasive practices, such as the use of live closed circuit television (CCTV), are not regulated by the *Privacy Act*.[147] It has been argued that consideration should be given to ensuring that agencies and organisations are not allowed to breach the spirit of the *Privacy Act* by avoiding making a record.[148]

Discussion Paper proposals

6.134 In IP 31, the ALRC asked whether the definitions, including the definition of record, in the *Privacy Act* were adequate and appropriate.[149] In response, the OPC made a number of suggestions for improving the definition of 'record', including amending the definition to make it 'stand alone' and to clarify its scope and application to developing technology. The OPC also recommended removing the phrase 'of a person' from 'a photograph or other pictorial representation of a person' on the basis that a photograph may be 'personal information' even though it is not a photograph of a person. For example, a photograph of a house may be personal information if it is kept together with other information that identifies the resident.[150]

6.135 In DP 72, the ALRC examined the approach adopted in the Victorian and Tasmanian legislation—that is, including the requirement that information be recorded as one element of the definition of 'personal information'. The problem with this approach is that information does not fall within the definition of 'personal information' and, therefore, is not covered by the privacy legislation in Victoria and

---

146 Information Privacy Bill 2007 (WA) cl 4.

147 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.19].

148 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [60]; 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, 7.

149 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 3–4.

150 The OPC also suggested that the definitions of 'record' and 'document' in the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth) should be harmonised.

Tasmania until it has actually been included in a record. This means, for example, that where a doctor or psychologist is collecting information orally from a patient or client during a consultation, the privacy legislation, including the collection principle, does not apply to that exchange because the information is not yet included in a record.

6.136 On the other hand, s 16B(1) of the *Privacy Act* provides that the Act applies to the collection of personal information if the information is *collected for inclusion* in a record or generally available publication. This approach ensures that information that is in the process of being collected for inclusion in a record—for example, by doctors and psychologists in the course of a consultation—but has not yet been recorded, is covered by the Act. The ALRC was of the preliminary view that this approach was preferable and should also be adopted in the amended *Privacy Act*.

6.137 In addition, the ALRC did not propose adopting the approach in the New South Wales *Privacy and Personal Information Act*, which does not expressly require that information be held in a record or collected for inclusion in a record. The ALRC noted Spiegelman CJ's view that the New South Wales Act should be interpreted to apply to information held, or collected for inclusion, in a record. It considered that such requirements should be set out expressly in legislation, rather than implied.

6.138 The ALRC further proposed that the *Privacy Act* should be limited to those situations in which information is held or collected for inclusion in a record. The ALRC noted that the Victorian Law Reform Commission is currently examining surveillance in public places, including live CCTV surveillance, as part of a larger inquiry into privacy. It is anticipated that the recommendations resulting from that inquiry will be considered by the Standing Committee of Attorneys-General. Other invasions of privacy involving personal information may be caught by the statutory cause of action for a serious invasion of privacy.[151]

6.139 The term 'record' is defined in the *Acts Interpretation Act*. It includes 'information stored or recorded by means of a computer'. The ALRC noted that this definition may not be sufficient in the context of the *Privacy Act.* It does not give an indication of the intended broad scope of the *Privacy Act*, which is not limited to information stored on computer. On this basis, the ALRC proposed that the term be defined separately in the *Privacy Act*, including a reference to information stored in electronic or other forms. The ALRC proposed that the definition of record in the *Privacy Act* be inclusive rather than exhaustive.

6.140 The ALRC considered the OPC's submission that the definition of 'record' in the *Privacy Act* should 'stand alone' and that it is undesirable to rely on the definition of 'document' in the *Acts Interpretation Act*. While there are valid arguments to support both the current approach and developing a 'stand alone' definition, on balance the ALRC proposed that the definition continue to rely on the *Acts Interpretation Act*.

---

151 Rec 74–1.

The long title of that Act is 'An Act for the Interpretation of Acts of Parliament and for Shortening their Language'. The ALRC expressed the preliminary view that it is appropriate to rely on the definitions provided in that Act unless the Australian Parliament intends a particular term to have a meaning that is different from the meaning set out in the *Acts Interpretation Act*. This promotes consistency and brevity in federal legislation.

6.141 The ALRC agreed with the OPC that photographs or other pictorial representations should be covered by the term 'record' in the *Privacy Act* and that they should not be limited by the phrase 'of a person'. This can be achieved by relying on the definition of 'document' in the *Acts Interpretation Act*, which includes 'any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device'. The term 'images' is wide enough to cover photographs and other pictorial representations.

6.142 The ALRC proposed, therefore, that the first inclusive part of the definition of 'record' in the *Privacy Act* should be amended to include a document, as defined by the *Acts Interpretation Act*, and information stored in electronic or other forms.[152]

Submissions and consultations

6.143 In response to DP 72, the OPC again suggested that the definition should 'stand alone' to ensure it is accessible and easily understood. The OPC was also of the view that consistent definitions of 'record' and 'document' should be developed for the purposes of the *Privacy Act*, the *Archives Act* and the FOI Act. In addition, the OPC was of the view that the definition of 'record' should continue to refer expressly to photographs and pictorial representations despite the ALRC's view that the definition of 'document' in the *Acts Interpretation Act* was broad enough to include them. The OPC was concerned that it may not be clear that 'document' is defined elsewhere to include photographs and pictures.[153]

6.144 A number of stakeholders expressed support for the changes to the definition of 'record' proposed in DP 72.[154] PIAC supported the proposed definition but expressed the view that it should be made clearer that the definition is an inclusive one, and that it

---

152 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–8.

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

154 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

relies on the definition of 'document' in the *Acts Interpretation Act*.[155] The Cyberspace Law and Policy Centre also expressed support for the ALRC's proposed definition but suggested that there may also be a need to clarify that 'a person' cannot constitute an 'other form' of storage of information.

> A person should not be a 'record' of their own biometric data, and nor should a person be regarded as 'storage' of everything that they know. The latter possibility would defeat the purpose of the general restriction of the Act's operation to personal information stored in records, excluding information only 'stored' in a person's mind.[156]

6.145 The Law Society of New South Wales suggested that the definition should be amended to read a document or 'information however stored or retained and not destroyed'.[157]

ALRC's view

6.146 The ALRC has again considered the wisdom of relying on the definition of 'document' in the *Acts Interpretation Act.* The ALRC notes that in a recent Drafting Direction the Office of Parliamentary Counsel has indicated that:

> Generally, if a particular expression is defined in an existing provision and you want to use that same expression with that defined meaning in another provision, you should consider repeating the whole of that definition rather than referring to the existing provision (even if this involves repeating large amounts of text). This is because it avoids the need for the reader to access another provision in order to find out the meaning of that expression.[158]

6.147 On the other hand, the Office of Parliamentary Counsel have also stated that:

> However, if you want to use an expression that is consistently used across the statute book with the same meaning, it may be preferable for the new provision to refer to the existing provision in which that expression is defined. This provides for greater consistency across the statute book by ensuring that the expression will always have the same meaning when used in various provisions. If the meaning of that expression needs to be changed across the statute book, it is easier to do so by amending a single definition to which all other provisions refer.[159]

6.148 Again, on balance, and for the reasons discussed above, the ALRC has come to the view that it is appropriate to rely on the definition of 'document' in the *Acts Interpretation Act.* The recommendation below refers expressly to the *Acts Interpretation Act* to make this clear. This approach leaves open the possibility, suggested by the OPC, that the use of the term 'document' in the *Privacy Act*, the FOI Act and the *Archives Act* may be brought into line. Although the FOI Act currently

---

155 *Acts Interpretation Act 1901* (Cth) s 25.
156 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
157 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.
158 Australian Government Office of Parliamentary Counsel, *Drafting Direction No 1.5: Definitions* (2008), [37].
159 Ibid, [38].

includes a separate definition of 'document', it would be possible to ensure consistency across all these Acts by amending the FOI Act so that it, too, relies on the definition of 'document' in the *Acts Interpretation Act*.

6.149 The ALRC has made one small change to the proposal in DP 72, that is, a change from 'information stored in electronic or other form' to 'information stored in electronic or other format'. This indicates that the definition of 'record' in the *Privacy Act* is not intended to capture information stored in a human body or brain.

Recommendation 6–6 The definition of 'record' in the *Privacy Act* should be amended to make clear that a record includes:

(a) a document (as defined in the *Acts Interpretation Act 1901* (Cth)); and

(b) information stored in electronic or other format.

Generally available publications

6.150 The definition of 'record' in the *Privacy Act* excludes a range of things such as items kept in libraries, art galleries or museums for reference, study or exhibition; a range of Commonwealth archival records, including those in the open access period; documents in the memorial collection of the Australian War Memorial and letters and other articles in the course of transmission by post. There were very few concerns raised with these elements of the definition, although Australia Post noted the importance of the exclusion of postal articles.[160] The ALRC does not recommend any changes to these elements.

6.151 The definition of 'record' in the *Privacy Act* also excludes 'generally available publications'—that is, 'a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public'. It is important to note, however, that the collection of personal information for inclusion in a generally available publication is regulated by the privacy principles.[161]

6.152 The OPC commented in its submission that:

> The Office notes that the phrase 'generally available publication' may appear to apply only to publications that do not involve fees for access. However, access to generally available publications is not necessarily free. For example, the National Insolvency Index is accessible only by subscribers who pay to view the Index.

160 Australia Post, *Submission PR 445*, 10 December 2007.
161 *Privacy Act 1988* (Cth) ss 14, 16B.

> For this reason, the Office believes that the definition would benefit from the clarification that a generally available publication is generally available even where payment of a fee is necessary to access the information.[162]

6.153 In DP 72, the ALRC proposed that the definition of 'generally available publication' be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.

Submissions and consultations

6.154 A number of stakeholders expressed support for this proposal.[163] The Queensland Government noted that it has always considered a publication to be generally available under Information Standard 42[164]—which regulates the handling of personal information in the Queensland public sector—whether or not a fee was payable.[165]

ALRC's view

6.155 The ALRC notes that a great number of generally available publications are only available for a fee, including those expressly included in the current definition such as books and magazines. The ALRC sees merit in clarifying that a publication is 'generally available' whether or not a fee is charged for access to the publication.

---

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

163 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 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; 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; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

164 Queensland Government, *Information Standard 42—Information Privacy* (2001).

165 Queensland Government, *Submission PR 490*, 19 December 2007.

Recommendation 6–7 The definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.

7. Privacy Beyond the Individual

Contents

Introduction

7.1 The *Privacy Act 1988* (Cth) only protects the privacy rights of individuals. This means that entities, such as groups of people and corporations, are unable to obtain direct protection of the Act. In this chapter, the ALRC examines whether this limitation is necessary and desirable. With particular reference to Indigenous groups, the ALRC considers whether the protection of the Act should extend to groups of people who are unified by a common race, ethnicity, culture or other characteristic. The ALRC also considers whether the protection of the Act should extend to organisations, partnerships, corporations and other such collective entities.

Privacy and group rights generally

Current application of the *Privacy Act* to groups

7.2 The *Privacy Act* explicitly protects 'individuals'.[1] Section 6(1) defines 'individual' as 'a natural person'.[2] The omission of groups from the ambit of the Act is consistent with the ALRC's 1983 report on privacy law (ALRC 22). In ALRC 22, the ALRC decided not to consider the notion of group privacy on the basis that it was outside the scope of the Inquiry. The ALRC noted, however, that corporate and group claims to privacy were 'of such complexity as to merit a separate and major study'.[3]

7.3 The decision to limit the Act's protection to individuals is reflected in the Preamble to the *Privacy Act*, which makes reference to human rights, and specifically to those guaranteed in the *International Covenant on Civil and Political Rights* (ICCPR).[4] The Preamble also refers to Australia's obligations at international law 'to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence' and to protect 'privacy and individual liberties'.

7.4 Currently, the *Privacy Act* applies if an individual suffers a breach of his or her privacy as a consequence of the individual's membership of a group. In some situations, however, it can be difficult to determine whether a privacy interest relates to a natural person or to a group. Hypothetical examples of these types of situations were given in ALRC 22:

> Should John Brown, who is entitled to access to his credit record, also be entitled to access to that of John Brown Pty Ltd? Should John Brown Pty Ltd be allowed access to records about John Brown, and about itself? Should Dr Fred Smith, whom everyone in the neighbourhood knows is the real person behind the corporate veil of Local Medical Services Pty Ltd, be entitled to access to information about both his corporation and himself?[5]

Protection of group rights in international law

7.5 The majority of the foundational international instruments that form the basis of international and domestic Australian human rights law do not provide for the direct protection of group rights.[6] To date, the Organisation for Economic Co-operation and Development (OECD) has not gone so far as to state that it is necessary to provide specific privacy protections for certain groups of people. The Explanatory

---

1 *Privacy Act 1988* (Cth) pt III div 1.

2 This is consistent with the definition in the Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 1(b).

3 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [27].

4 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

5 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [29].

6 Arguably, an exception is *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 27.

Memorandum to the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) states that 'it is debatable to what extent people belonging to a particular group (ie mentally disabled persons, immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group'.[7] The vast majority of overseas jurisdictions do not attempt to protect the privacy rights of groups.[8]

7.6 On the other hand, group rights are recognised in some other international instruments—particularly more recent instruments such as the *African Charter of Human and Peoples' Rights*.[9] Additionally, the *Declaration on the Rights of Indigenous Peoples* states that 'Indigenous peoples have … the right to maintain, protect, and have access in privacy to their religious and cultural sites'.[10] While the Declaration was adopted by 143 members of the United Nations General Assembly, Australia was one of four states that voted against its adoption.[11]

7.7 Finally, international human rights law recognises that certain ethnic and cultural groups within a community may have particular needs that require protection. For example, the ICCPR recognises the need to protect the cultural, religious and language rights of certain ethnic and cultural groups. Article 27 states:

> In those States in which ethnic, religious or linguistic minorities exist, persons belonging to such minorities shall not be denied the right, in community with the other members of their group, to enjoy their own culture, to profess and practise their own religion, or to use their own language.

Extension of the *Privacy Act* to groups?

7.8 In light of the above, the ALRC asked in the Issues Paper, *Review of Privacy* (IP 31), whether the Act should be amended to accommodate a 'collective' or 'group' right to privacy. The ALRC noted that there is some precedent for explicit privacy

---

7 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [32].

8 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 179, 192–198.

9 *African Charter on Human and Peoples' Rights*, 27 June 1981, OAU Doc CAB/LEG/67/3 rev 5, (entered into force generally on 21 October 1986), eg, arts 19–24.

10 *United Nations Declaration on the Rights of Indigenous Peoples*, GA Res 61/295, 61st sess, UN Doc A/RES/61/295, (2007), art 12(1).

11 Before the 2007 federal election, the Australian Labor Party indicated its support for the Declaration: J Macklin (Shadow Minister for Indigenous Affairs and Reconciliation), 'International Declaration On The Rights Of Indigenous Peoples' (Press Release, 14 September 2007).

protection at common law for Indigenous groups in Australia.[12] Northern Territory legislation also provides for limited privacy protection.[13]

7.9 In Discussion Paper 72, *Review of Australian Law* (DP 72), the ALRC did not foreclose the possibility of such an amendment to the *Privacy Act*, but expressed the view that the Act should not be extended to provide direct protection to Indigenous or other racial, cultural or ethnic groups, or commercial entities.[14]

7.10 With regard to the privacy of Indigenous groups, the ALRC expressed the view that the development of privacy protocols that respond to the particular privacy needs of those groups, rather than an amendment to the *Privacy Act*, was the more effective and appropriate solution.

Submissions and consultations

Groups generally

7.11 There was limited support for the legislative extension of privacy rights to groups.[15] Associate Professor Lee Bygrave argued that while much of the literature on privacy and its value is almost exclusively concerned with the interests of individuals:

> It is fairly easy to establish that the core principles of the *Privacy Act* are *logically* capable of being extended to protect data on collective entities. Further, it is fairly easy to establish that collective entities are capable of sharing most, if not all, of the interests of data subjects which the *Privacy Act* directly or indirectly safeguards …[16]

7.12 Bygrave counselled against treating 'collective entities … as an undifferentiated mass' because they do not all 'play the same economic, political, legal and social roles, nor have the same goals and resources'.[17] He concluded that, on balance, all countries should seriously consider giving collective entities some data protection rights.[18]

---

12 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [1.50]–[1.54]. See, eg, *Aboriginal Sacred Sites Protection Authority v Maurice; Re the Warumungu Claim* (1986) 10 FCR 104, 107. See also the discussion of the relevant case law in Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [19.125]–[19.126].

13 *Information Act 2002* (NT), ss 50, 56. See also, National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [1.10]. The National Statement is discussed in detail in Chs 64–66.

14 The extension of privacy rights to corporations or commercial entities is discussed later in this chapter.

15 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; L Bygrave, *Submission PR 92*, 15 January 2007.

16 L Bygrave, *Submission PR 92*, 15 January 2007 (emphasis in original).

17 Ibid.

18 Ibid, citing L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 297.

7.13 A clear majority of stakeholders, however, opposed any legislative extension of privacy rights to groups.[19] A number of stakeholders observed that privacy is a fundamental human right, which is based on protecting the dignity and autonomy of individuals. As such, it was argued that privacy rights cannot logically be extended to groups.[20] Given that the constitutional foundation of the *Privacy Act* relies partly on the fact that it implements art 17 of the ICCPR, the Office of the Information Commissioner Northern Territory expressed concern that any extension of the Act to protect groups might undermine its constitutional validity.[21]

Indigenous or other racial, cultural or ethnic groups

7.14 Several stakeholders opposed extending privacy law to provide direct and specific protection to Indigenous or other racial, ethnic or cultural groups.[22] The Office of the Information Commissioner Northern Territory expressed concern that such an extension could be used in the name of a group, but 'against the interests of individual group members'.[23] The Office of the Privacy Commissioner (OPC) submitted that such an extension would cause a number of practical problems. For example, it would be

---

19 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Telstra, *Submission PR 185*, 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; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Law Society of New South Wales, *Submission PR 146*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

20 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Telstra, *Submission PR 185*, 9 February 2007; Australian Competition and Consumer Commission, *Submission PR 178*, 31 January 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Confidential, *Submission PR 165*, 1 February 2007; 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; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Law Society of New South Wales, *Submission PR 146*, 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

21 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

22 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Australian Bureau of Statistics, *Submission PR 383*, 6 December 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156*, 31 January 2007; Confidential, *Submission PR 143*, 24 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; AXA, *Submission PR 119*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007.

23 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

difficult to determine which ethnic groups should be afforded additional privacy protection.[24]

7.15 The Australian Government Department of Health and Ageing submitted that such an extension of the Act is unnecessary because the privacy principles already recognise cultural sensitivities adequately by

> requiring the reasonable expectations of the individual concerned to be taken into account when using or disclosing personal information for secondary purposes. Any 'cultural sensitivity' would be one of the matters to be considered in weighing up whether the individual would reasonably expect his or her personal information to be used or disclosed.[25]

7.16 The Australian Government Department of Families, Communities and Indigenous Affairs submitted that any extension of the Act, if it were limited to Indigenous groups, would be inconsistent with the protection afforded to other cultural groups and could cause difficulties for agencies in fulfilling their statutory duties.[26]

7.17 Some stakeholders supported extending privacy law to provide direct protection to Indigenous or other groups.[27] The Centre for Law and Genetics stated that such an expansion would be consistent with the 'underlying ethical rationale for privacy protection, which is based in notions of human dignity and autonomy'.[28]

ALRC's view

7.18 Any extension of the right to privacy to a group would cause problems of logic, law and policy. It would require a fundamental and radical change to the scope and operation of the *Privacy Act* to provide direct protection to the privacy of groups. This does not mean, however, that such a realignment of the *Privacy Act* cannot or should not occur, if there is a compelling case for such a realignment.

7.19 Without detracting from the universality of human rights, there is relatively broad acceptance that particular rights can attach to members of a group of people united by, for example, ethnic origin or religion.[29] That is, it is generally recognised that the individuals from certain groups may have needs that are peculiar to those

---

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

25 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

26 Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007. See also Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

27 Queensland Government, *Submission PR 242*, 15 March 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.

28 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

29 This is exemplified in instruments such as Africa's principal human rights treaty, the *African Charter on Human and Peoples' Rights*, 27 June 1981, OAU Doc CAB/LEG/67/3 rev 5, (entered into force generally on 21 October 1986). The Preamble to the Charter recognises that 'fundamental human rights stem from the attributes of human beings which justifies their national and international protection and on the other hand that the reality and respect of peoples' rights should necessarily guarantee human rights'.

groups.[30] This may result from a group suffering historical discrimination or disadvantage. Alternatively, it may flow from the particular cultural beliefs or requirements of a group.[31]

7.20 Australian law has long recognised that, in order to ensure that all members of the community enjoy substantive equality, it is sometimes necessary to make laws that are targeted towards individuals who share particular characteristics.[32] For example, the *Racial Discrimination Act 1975* (Cth) permits the adoption of 'special measures', which operate as follows:

> Special measures taken for the sole purpose of securing adequate advancement of certain racial or ethnic groups or individuals requiring such protection as may be necessary in order to ensure such groups or individuals equal enjoyment or exercise of human rights and fundamental freedoms shall not be deemed racial discrimination, provided, however, that such measures do not, as a consequence, lead to the maintenance of separate rights for different racial groups and that they shall not be continued after the objectives for which they were taken have been achieved.[33]

7.21 Instead of amending the *Privacy Act*, there are other, more appropriate, methods of dealing with the privacy rights of groups.[34] The vast majority of stakeholders opposed extending the Act's protection directly to cover Indigenous or other racial, cultural or ethnic groups. As noted in submissions and consultations, such an extension of the *Privacy Act* could have undesirable consequences. For example, it could result in a group asserting privacy rights in a way that conflicts with the interests of individual members of the group. While it may be possible to reconcile conflicts between individual and collective rights in some circumstances,[35] in the ALRC's view such conflicts would be particularly difficult to resolve in the context of privacy protection.

Traditional laws and customs of Indigenous groups

7.22 In this section, the ALRC focuses on the privacy of Indigenous groups. During the course of this Inquiry, a number of stakeholders expressed concerns about the privacy of Indigenous groups, rather than other identified racial, ethnic or cultural groups. Consequently, the ALRC has focused on the privacy of Indigenous groups.

---

30 See, eg, International Covenant on Civil and Political Rights, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 27.

31 See, eg, D Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd ed, 2002), 13–14.

32 See, eg, R Piotrowicz and S Kaye, *Human Rights: International and Australian Law* (2000), [12.23].

33 See *Racial Discrimination Act 1975* (Cth) s 8(1), incorporating *International Convention on the Elimination of all Forms of Racial Discrimination*, 7 March 1966, [1975] ATS 40, (entered into force generally on 4 January 1969), art 1(4).

34 In the following section, the ALRC recommends that the OPC should encourage and assist agencies and organisations to develop and publish protocols, in consultation with Indigenous groups and representatives, to address the particular privacy needs of Indigenous groups: Recommendation 7–1.

35 See, eg, L McDonald, 'Can Collective and Individual Rights Coexist?'' (1998) 22 *Melbourne University Law Review* 310, 323–336. See also United Nations Human Rights Committee, *Kitok v Sweden: Communication No 197/1985*, UN Doc A/43/40 (1988).

This in no way suggests that the OPC should refrain from developing and publishing guidance on the privacy rights of other racial, cultural or ethnic groups. Rather, it indicates that the views expressed by stakeholders in submissions and consultations were specifically directed to the privacy of Indigenous groups.

7.23 In previous Inquiries, the ALRC has noted concerns about the adequacy of legal protection for the cultural rights of Indigenous groups.[36] Several stakeholders noted the particular interaction between Anglo-Australian laws and the traditional laws and customs of Indigenous groups.[37]

7.24 For example, under the traditional laws and customs of Indigenous groups certain information may be viewed or disclosed only to a defined category of people—such as the women of a particular Indigenous group.[38] In addition, it is often contrary to the traditional laws and customs of Indigenous groups to broadcast the name or image of an Indigenous person who is deceased.[39]

7.25 On one view, such laws and customs relate to information privacy rights because the information in question is intimately connected to the identity, dignity and autonomy of Indigenous people—individually, collectively or both. On another view, these rules more closely resemble intellectual property or cultural heritage laws.[40] For example, Indigenous laws and customs may be expressed through music, dance, song, ceremonies, symbols and designs, narratives and poetry. Scientific, agricultural, technical and ecological knowledge, and knowledge related to and contained in items of moveable and immoveable cultural property, also form part of Indigenous laws and customs.[41]

7.26 In *Western Australia v Ward* it was argued that Indigenous cultural knowledge of land is 'akin to a new species of intellectual property'.[42] The inescapable problem, however, is that existing traditional laws and customs of Indigenous people do not fit neatly within the Anglo-Australian legal system's traditional conceptualisations of privacy or of intellectual property. In *Ward*, Kirby J noted that 'the established laws of intellectual property are ill-equipped to provide full protection of the kind sought'.[43]

---

36 See, eg, Australian Law Reform Commission, *The Recognition of Aboriginal Customary Laws*, ALRC 31 (1986), [213]; Australian Law Reform Commission, *Designs*, ALRC 74 (1995), [1.17].

37 See, eg, Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007; New South Wales Aboriginal Justice Advisory Council, *Submission PR 501*, 20 December 2007; Queensland Government, *Submission PR 242*, 15 March 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.

38 See, eg, *Wilson v Minister for Aboriginal & Torres Strait Islander Affairs* (1996) 189 CLR 1.

39 See, eg, Special Broadcasting Service, *SBS Codes of Practice* (2006), [1.3.1].

40 See, eg, S Gray, 'Imagination, Fraud and the Cultural Protocols Debate: A Question of Free Speech or Pornography' (2004) 9 *Media & Arts Law Review* 23, 23.

41 T Janke, *Our Culture: Our Future—Report on Australian Indigenous Cultural and Intellectual Property Rights* (1998) Australian Institute of Aboriginal and Torres Strait Islander Studies and the Aboriginal and Torres Strait Islander Commission.

42 See *Western Australia v Ward* (2002) 213 CLR 1, [59], [582].

43 Ibid, [582].

There are many reasons for this disjuncture, beyond obvious differences in the relevant underlying norms. For example, unlike Anglo-Australian law, for some Indigenous groups law can be confidential or private.[44] Similarly, the traditional laws and customs of Indigenous groups often delineate between individual and group rights in a way that differs from the Anglo-Australian legal system. It has been observed that:

> Indigenous legal systems revolve around group rights and group control, whereas the Australian legal system has developed out of a more individualistic tradition, with greater emphasis on personal rights and freedoms.[45]

7.27 Several Australian Government inquiries have acknowledged the vexed question of how to protect adequately Indigenous cultural rights. In 1986, the ALRC released *The Recognition of Aboriginal Customary Laws* (ALRC 31). In that Report, the ALRC acknowledged that the sale of Aboriginal paintings and objects could breach Aboriginal customary laws.[46] In the ALRC's 1995 Report, *Designs* (ALRC 74), the ALRC expressed the view that the protection of traditional Aboriginal and Torres Strait Islander designs raises special issues 'that should not be dealt with in isolation from other issues arising out of Aboriginal art, culture and heritage'.[47] In both inquiries, the ALRC did not make recommendations on this issue, but noted that other government bodies were examining the matter.[48]

7.28 In 2007, an inquiry into the Indigenous visual arts and craft sector by the Senate Standing Committee for the Environment, Communications, Information Technology and the Arts considered some of these issues.[49] The Committee made several recommendations relating to the Indigenous arts sector, including that, 'recognising the complexity of the issues in this area, the Commonwealth introduce appropriate legislation to provide for the protection of Indigenous cultural and intellectual property rights'.[50]

Privacy protocols for Indigenous groups

7.29 A privacy protocol is a document that sets out how to respect the particular privacy rights and needs of a group or groups of people in certain situations. In DP 72, the ALRC proposed that the OPC, in conjunction with Indigenous and other ethnic

---

44 See, eg, the discussion in H McRae, G Nettheim and L Beacroft, *Indigenous Legal Issues* (1997), 133–134.

45 Ibid, 136.

46 Australian Law Reform Commission, *The Recognition of Aboriginal Customary Laws*, ALRC 31 (1986), [213].

47 Australian Law Reform Commission, *Designs*, ALRC 74 (1995), [1.17].

48 Australian Law Reform Commission, *The Recognition of Aboriginal Customary Laws*, ALRC 31 (1986), [213]; Australian Law Reform Commission, *Designs*, ALRC 74 (1995), [1.17].

49 Senate Standing Committee on Environment Communications Information Technology the Arts, *Indigenous Art—Securing the Future (Australia's Indigenous Visual Arts and Craft Sector)* (2007).

50 Ibid, rec 25.

groups, encourage and assist the creation of publicly available protocols that respond to the particular privacy needs of those groups.[51]

7.30 This section examines whether privacy protocols represent an appropriate mechanism to protect the privacy of Indigenous groups and, if so, how they should be implemented within the overall privacy regime recommended in this Report.

Protocols generally

7.31 Currently, there are protocols that set out the steps the media should take to protect the privacy of Indigenous and other ethnic or cultural groups.[52] Though generally expressed in mandatory language, these protocols are 'primarily ethical in nature'. They articulate 'levels of behaviour which indigenous people and communities expect of outsiders dealing with indigenous material',[53] and often suggest ways of protecting the 'honour and dignity' of Indigenous people that are portrayed in the media.[54]

Support for the development of privacy protocols

7.32 A number of stakeholders supported the creation of privacy protocols for Indigenous groups, and argued that they should be adopted widely.[55] SBS stated that its codes, Independent Indigenous Protocols and 1997 policy document, *The Greater Perspective*, all encourage 'respect for Indigenous culture and heritage, recognition of Indigenous cultural and intellectual property rights, maintenance of cultural integrity and respect for cultural beliefs, and respect for Indigenous individuals and communities'.[56] These documents

> include guidelines on consulting with Indigenous groups, and the need to take unique cultural considerations into account when creating content with Indigenous participants. The application of these protocols allow[s] for more positive collaborations with Indigenous communities, rather than the creation of a rigid framework which could serve to silence legitimate voices.[57]

7.33 Further, a number of stakeholders expressed support for the ALRC's proposal that the OPC, in conjunction with Indigenous and other ethnic groups, should

---

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

52 L Bostock, *The Greater Perspective: Protocol and Guidelines for the Production of Film and Television on Aboriginal and Torres Strait Islander Communities* (1997) SBS <www20.sbs.com.au/sbscorporate/media/documents/5315sbs_booklet.pdf> at 1 May 2008.

53 S Gray, 'Imagination, Fraud and the Cultural Protocols Debate: A Question of Free Speech or Pornography' (2004) 9 *Media & Arts Law Review* 23, 24.

54 See L Bostock, *The Greater Perspective: Protocol and Guidelines for the Production of Film and Television on Aboriginal and Torres Strait Islander Communities* (1997) SBS <www20.sbs.com.au/sbscorporate/media/documents/5315sbs_booklet.pdf> at 17 July 2007, 23.

55 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; SBS, *Submission PR 112*, 15 January 2007.

56 SBS, *Submission PR 112*, 15 January 2007.

57 Ibid.

encourage and assist the creation of publicly available protocols that respond to the particular privacy needs of groups.[58]

7.34 The OPC supported the proposal, noting that in 1998 it prepared guidance for agencies that handle the personal information of Indigenous people in the Northern Territory.[59]

7.35 Stakeholders suggested that the benefits of a regime involving privacy protocols developed by the OPC include: flexibility in the type and range of information that is protected;[60] the opportunity to consult widely with Indigenous groups and representatives about the nature of protected information;[61] and the potential to achieve uniformity across jurisdictions within Australia.[62]

Features of a regime involving privacy protocols

7.36 A number of stakeholders suggested that consultation with Indigenous stakeholders is necessary for the development of adequate privacy protocols.[63] National Legal Aid submitted that there may be a diversity of views within any Indigenous or cultural group.[64] The Public Interest Advocacy Centre (PIAC) expressed concern that the OPC has developed only one privacy protocol relating to Indigenous rights, and this was created nearly a decade ago. PIAC submitted that there should be a positive obligation on the OPC to consult with Indigenous representatives such as the Aboriginal and Torres Strait Islander Social Justice Commissioner, and relevant Indigenous groups, to review and update the existing protocol.[65] The Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) and the

---

58 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; 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; Legal Aid Queensland, *Submission PR 489*, 19 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.

59 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Privacy Commissioner, *Minding Our Own Business: Privacy Protocol for Commonwealth Agencies in the Northern Territory Handling Personal Information of Aboriginal and Torres Strait Islander People* (1998).

60 New South Wales Aboriginal Justice Advisory Council, *Submission PR 501*, 20 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.

61 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.

62 Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; E Orr, *Submission PR 346*, 22 November 2007.

63 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007; New South Wales Aboriginal Justice Advisory Council, *Submission PR 501*, 20 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.

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

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

Aboriginal and Torres Strait Islander Social Justice Commissioner advised the Inquiry of their willingness to be involved in such a consultation process.[66]

7.37 It was also suggested in submissions that education will be essential to ensure awareness about rights and obligations arising from the protocols. The Office of the Victorian Privacy Commissioner noted that Indigenous people currently are under-represented as complainants in Victoria and other jurisdictions.[67] PIAC submitted that issues of secrecy and privacy for Indigenous communities are not well understood.[68]

7.38 Some stakeholders suggested particular areas in respect of which privacy protocols for Indigenous groups should be introduced. These include child protection,[69] health, and the credit and telecommunications industries.[70]

7.39 It was also submitted that the introduction of privacy protocols should augment, rather than diminish, the privacy rights of Indigenous groups. Accordingly, compliance with a privacy protocol should not mean that an Indigenous individual loses the protection of privacy laws, such as that provided by the *Privacy Act*.[71]

Concerns about privacy protocols

7.40 A number of stakeholders questioned the efficacy of privacy protocols.[72] For example, the Law Council of Australia was of the view that a stronger legislative model for the privacy of Indigenous groups was required. It noted 'that the flexibility afforded by the high level principle approach associated with protocols … may not provide sufficient protection for the privacy rights of Indigenous groups'.[73] It was also submitted that the introduction of privacy protocols would lead to complexity within the privacy regime.[74]

7.41 The Aboriginal Justice Advisory Council (AJAC) submitted that 'protocols are useful but only to the extent that the provisions are understood, adhered to, and performed'.[75] AJAC noted that existing Australian laws, including laws relating to

---

66 Human Rights and Equal Opportunity Commission, *Submission PR 500,* 20 December 2007; Australian Institute of Aboriginal and Torres Strait Islander Studies, *Consultation PC 226*, Canberra, 12 December 2007.

67 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

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

69 E Orr, *Submission PR 346,* 22 November 2007.

70 Arts Law Centre of Australia, *Submission PR 450,* 7 December 2007.

71 See, eg, E Orr, *Submission PR 346,* 22 November 2007.

72 Law Council of Australia, *Submission PR 527,* 21 December 2007; New South Wales Aboriginal Justice Advisory Council, *Submission PR 501,* 20 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500,* 20 December 2007; Arts Law Centre of Australia, *Submission PR 450,* 7 December 2007; Contemporary Arts Organisations Australia, *Submission PR 384,* 6 December 2007; Artsource, *Submission PR 350,* 28 November 2007.

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

74 Insurance Council of Australia, *Submission PR 485,* 18 December 2007; Arts Law Centre of Australia, *Submission PR 450,* 7 December 2007.

75 New South Wales Aboriginal Justice Advisory Council, *Submission PR 501,* 20 December 2007.

intellectual property and cultural heritage, offered only limited protection for the rights of Indigenous groups. It submitted that *sui generis* (specific) legislation that protected all forms of Indigenous culture was required. Nevertheless, it supported the privacy protocols proposed by the ALRC 'as an interim measure or as a companion to other legislative/contractual measures'.[76]

7.42 The Arts Law Centre of Australia also supported the introduction of specific legislation that would protect Indigenous cultural heritage and intellectual property. It did not support the ALRC's proposal to introduce privacy protocols for groups of individuals, and submitted that

> there are numerous existing protocols in the intellectual property and cultural fields in relation to Indigenous communities. It has been our experience that these are insufficient and that Indigenous artists and communities receive little protection and are frequently exploited. None of the existing protocols are enforceable unless they are adopted in individual contracts. Where voluntary protocols are adopted, they are adopted by participants who are focussed on appropriate conduct.[77]

7.43 The Human Rights and Equal Opportunity Commission (HREOC) suggested that, to address concerns about non-compliance with protocols, the ALRC should consider amending the *Privacy Act* to give legal effect to rights and obligations arising under such protocols. For example, a privacy protocol could be approved by the OPC as a 'code' under Part IIIAA.[78]

ALRC's view

7.44 Currently, the most appropriate means of ensuring greater protection of group information that is of particular significance to Indigenous groups is for the OPC to encourage and assist agencies and organisations to create publicly available protocols that respond to the privacy needs of these groups.

7.45 The creation of privacy protocols would allow the principles set out in the *Privacy Act* to remain at a relatively high level, thereby avoiding an overly prescriptive approach to privacy regulation.[79] This, in turn, will ensure that the Act retains its flexibility, allowing it to be applied in a broad range of circumstances. The development of privacy protocols will encourage those collecting group information to consult and negotiate with the relevant members of an Indigenous group before handling information that is culturally sensitive.[80]

---

76 Ibid.
77 Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007.
78 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.
79 See Rec 18–1.
80 S Gray, 'Imagination, Fraud and the Cultural Protocols Debate: A Question of Free Speech or Pornography' (2004) 9 *Media & Arts Law Review* 23, 35; Special Broadcasting Service, *SBS Codes of Practice* (2006), [1.3.1]; T Janke and N Guivarra, *Listen, Learn and Respect: Indigenous Cultural*

7.46 Privacy protocols should be developed in consultation with Indigenous groups and representatives to ensure that they are appropriate and effective. Indigenous groups, and representatives such as AIATSIS and the Aboriginal and Torres Strait Islander Social Justice Commissioner, are uniquely positioned to advise on the particular areas in which such protocols should be developed. These areas might include, for example, child protection,[81] the media, or regimes for access to the information of deceased individuals.[82]

7.47 Further, the ALRC agrees that it is essential that Indigenous groups, agencies and organisations are informed about how privacy protocols are developed, and any rights and obligations that may arise from the development of such protocols. Accordingly, the OPC should promote awareness of the privacy issues relating to Indigenous groups.

7.48 In recommending the development of privacy protocols, the ALRC is mindful of the concerns expressed about the efficacy of protocols in protecting the privacy rights of Indigenous groups, and acknowledges that protocols may not present the best comprehensive, long-term solution. In addition, the ALRC acknowledges that reform of existing laws would not provide the holistic protection of Indigenous cultural rights sought by some stakeholders to this Inquiry. For example, while the *Privacy Act* might protect privacy of some sacred knowledge of Indigenous groups, it could not provide rights for control of access to Indigenous sacred sites, nor would it allow groups to exercise control over recordings of cultural customs and expressions. Similarly, other laws, such as native title and intellectual property, have only limited capacity to protect Indigenous cultural rights.

7.49 In the current Inquiry, the ALRC did not receive sufficient information to recommend that the Australian Government introduce a legislative framework for the protection of a range of cultural rights relating to the traditional laws and customs of Indigenous groups—which might include rights akin to privacy, cultural heritage and intellectual property rights. Further, in the ALRC's view, such a recommendation would be outside the Terms of Reference for this Inquiry.

7.50 A further inquiry should be undertaken, however, to determine whether the Australian Government should introduce a rights framework for the traditional laws and customs of Indigenous groups. Such an inquiry should involve extensive consultation with Indigenous groups and representatives, and could consider: whether such a framework is desirable; if so, what types of rights should be protected through such a framework; the most appropriate mechanism through which to recognise such

---

Protocols and Radio (2006) Australian Film Television and Radio School, 17; L Bostock, *The Greater Perspective: Protocol and Guidelines for the Production of Film and Television on Aboriginal and Torres Strait Islander Communities* (1997) SBS <www20.sbs.com.au/sbscorporate/media/documents/5315sbs_booklet.pdf> at 17 July 2007, 25.

81 E Orr, *Submission PR 346*, 22 November 2007.

82 The privacy of deceased individuals is discussed further in Ch 8.

rights; the methods for establishing rights and determining disputes among rights-holders; and the relationship between such a framework and other Australian laws.

Recommendation 7–1 The Office of the Privacy Commissioner should encourage and assist agencies and organisations to develop and publish protocols, in consultation with Indigenous groups and representatives, to address the particular privacy needs of Indigenous groups.

Recommendation 7–2 The Australian Government should undertake an inquiry to consider whether legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take.

Corporations and commercial entities

A right to privacy?

7.51 In DP 72, the ALRC expressed the preliminary view that the *Privacy Act* should not be extended to provide direct protection to corporations and other commercial entities. This view was based primarily on the following factors: such an extension would be inconsistent with the concept of privacy as a human right; it would conflict with fundamental principles of corporations law; and there is no demonstrable need for such an extension.[83] This section considers whether privacy rights should be extended to protect the privacy of corporations.

7.52 Some have suggested that the *Privacy Act* should be extended to protect the putative privacy rights of corporations. Proponents of this view maintain that a right to privacy traditionally has been inextricably, but erroneously, linked to autonomy and dignity.[84] Shorn of this link, they see no reason why the same privacy rights enjoyed by natural persons should not be extended to corporations.[85] Alternatively, it has been argued that protecting the privacy rights of a corporation ensures the protection of the autonomy of the individuals that constitute the corporation.[86]

---

83 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [1.108]–[1.112].

84 See, eg, C Doyle and M Bagaric, 'The Right to Privacy and Corporations' (2003) 31 *Australian Business Law Review* 237, 246–250; L Bygrave, 'A Right to Privacy for Corporations? Lenah in an International Context' (2001) *Privacy Law and Policy Reporter* 58.

85 C Doyle and M Bagaric, 'The Right to Privacy and Corporations' (2003) 31 *Australian Business Law Review* 237, 250.

86 N Witzleb, 'The Protection of Corporations from Intrusive Media: A German Perspective' (2006) 13(1) *E-Law—Murdoch University Electronic Journal of Law* 77, 104.

7.53 In the United States, the purpose of privacy law has traditionally been seen as 'protecting the *individual* and not social relationships'.[87] Professor William Prosser's *Restatement of the Law on Torts* sees privacy as denoting 'a personal right, peculiar to the individual whose privacy is invaded'.[88] Reasons for excluding corporations from the protection of US privacy law are that: corporations lack emotional traits; there is insufficient judicial precedent on the issue; and corporations have alternative remedies available to them.[89] It has been noted, however, that collective entities may have rights that resemble privacy rights, such as the right to the exclusive use of its name or identity in certain circumstances and rights under the law of unfair competition.

> A corporation, partnership or unincorporated association has no personal right of privacy. It has therefore no cause of action for [breach of privacy]. It has, however, a limited right to the exclusive use of its own name or identity in so far as they are of use or benefit, and it receives protection from the law of unfair competition. To some limited extent this may afford it the same rights and remedies as those to which a private individual is entitled …[90]

7.54 The data protection laws of some jurisdictions, such as Austria, Italy, Argentina and Switzerland, expressly protect the privacy of collective entities.[91] The South African Law Reform Commission (SALRC) also has expressed a preliminary view that privacy law should provide some protection to both types of legal person (that is, natural persons and entities such as corporations). The SALRC acknowledged, however, that it would be inappropriate to provide the same level of protection to collective entities as is afforded to natural persons.[92]

Submissions and consultations

7.55 A large number of stakeholders opposed extending the *Privacy Act* to protect corporations and other commercial entities.[93] Several stakeholders pointed out that corporate and commercial entities can use other laws, such as the action for breach of confidence and statutory protection of intellectual property, to protect their

---

87 N Richards and D Solove, 'Privacy's Other Path: Recovering the Law of Confidentiality' (2007) 96 *Georgetown Law Journal* 123, 173.

88 *Restatement of the Law, 2nd, Torts 1977* (US), § 652I(a).

89 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 193.

90 *Restatement of the Law, 2nd, Torts 1977* (US), § 652I(c).

91 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 179–180.

92 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), [3.4.8].

93 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Competition and Consumer Commission, *Submission PR 178*, 31 January 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Confidential, *Submission PR 165*, 1 February 2007; Law Society of New South Wales, *Submission PR 146*, 29 January 2007; Confidential, *Submission PR 143*, 24 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; AXA, *Submission PR 119*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

information.[94] Further, it was suggested that such an extension would lead to commercial entities operating less transparently.[95] One stakeholder stated that this would inhibit proper corporate governance.[96] The Australian Competition and Consumer Commission submitted that such an extension could allow some corporate entities to 'delay or distract when subject to investigation or other enforcement action'.[97]

7.56 While generally opposed to the extension of privacy law beyond natural persons, the Australian Bankers' Association submitted that, given incorporated entities are no longer able to protect their reputation through defamation, 'arguably a limited right of privacy should be accorded to corporations in relation to the disclosure of defamatory material harmful to the reputation of corporations'.[98]

7.57 A small number of stakeholders suggested that it may be appropriate to extend privacy law to protect corporations and other commercial entities.[99] Although noting that a small, but significant, number of jurisdictions protect the privacy rights of collective entities such as corporations, Bygrave suggested that this is partly the result of the 'pre-existing legal traditions' in those jurisdictions. He noted that a 'fundamental premise of the Austrian, Swiss and South African legal systems, for example, is that legal persons are to be treated as far as possible in the same way as natural persons'.[100]

ALRC's view

7.58 It is not appropriate to extend privacy protection to corporations and other commercial entities. First, as already discussed, the *Privacy Act* is premised on the notion that privacy is a human right. Extending the protection of a human right to an entity that is not human is inconsistent with the fundamental approach of Australian privacy law.[101] There is no compelling reason to risk distorting the theoretical basis of the *Privacy Act* by making such a change, because there are more appropriate avenues

---

94 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Competition and Consumer Commission, *Submission PR 178*, 31 January 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Confidential, *Submission PR 165*, 1 February 2007; Law Society of New South Wales, *Submission PR 146*, 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

95 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Confidential, *Submission PR 165*, 1 February 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

96 Confidential, *Submission PR 165*, 1 February 2007.

97 Australian Competition and Consumer Commission, *Submission PR 178*, 31 January 2007.

98 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

99 W Caelli, *Submission PR 99*, 15 January 2007; L Bygrave, *Submission PR 92*, 15 January 2007.

100 L Bygrave, *Submission PR 92*, 15 January 2007.

101 See, R Piotrowicz and S Kaye, *Human Rights: International and Australian Law* (2000), 3; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 226–227, 258, 279. Callinan J was more equivocal on this point: see 326–327.

for protecting the information rights of commercial entities. These include avenues provided by statutory protection of intellectual property and actions for breach of confidence.

7.59 Secondly, such an extension of the Act could undermine some of the fundamental principles of commercial law. This problem is particularly acute in relation to corporations, which are obliged to operate in a relatively transparent way. Moreover, part of the rationale for adopting the structure of a corporation is precisely to create a barrier between the identity of the corporation and the identity of the persons who establish, run and own it. To assign rights to the corporation would require a choice: either those rights must be assigned to the corporation itself, which would make it necessary to re-conceptualise some fundamental aspects of human rights law; or one must 'pierce the corporate veil', assigning those rights to the persons behind the corporation, which would make it necessary to re-conceptualise some aspects of corporations law.

7.60 As noted above, the vast majority of stakeholders opposed such a significant change to these fundamental tenets of the Act. This fact, coupled with the other points noted above, reinforce the ALRC's conclusion that such an extension of the *Privacy Act* is neither necessary nor desirable.

8. Privacy of Deceased Individuals

Contents

Introduction

8.1 Paul Roth has noted that:

> It is normally accepted that in law, deceased persons have no privacy interests. This is presumably on the basis that the *raison d'être* for privacy protection no longer exists, since dead people can feel no shame or humiliation. The underlying common law principle here is much the same as in the law of defamation, which in most jurisdictions does not countenance civil actions that seek to vindicate the reputation of the dead.[1]

8.2 In this chapter, the ALRC considers whether the *Privacy Act 1988* (Cth) should be amended to provide protection for the personal information of deceased individuals.

---

1 P Roth, 'Privacy Proceedings and the Dead' (2004) 11 *Privacy Law & Policy Reporter* 50.

Although a deceased individual may 'feel no shame or humiliation', there are sound public policy reasons to extend and amend certain of the model Unified Privacy Principles (UPPs) to create a set of provisions that apply to the personal information of deceased individuals. The ALRC recommends provisions to regulate the use and disclosure of the personal information of deceased individuals; access by third parties; data quality; and data security.

8.3 In the ALRC's view, the protection provided by the *Privacy Act* is analogous to the protection provided by legal duties of confidentiality that, unlike a right to sue for defamation, do survive the death of the individual. The provisions recommended in this chapter are intended to ensure that living individuals are confident to provide personal information, including sensitive information, in the knowledge that the information will not be disclosed in inappropriate circumstances after they die. The provisions are also intended to protect living relatives and others from distress caused by the inappropriate handling of a deceased individual's personal information and to provide a right of access to that information for family members and others where such access is reasonable.

8.4 In Chapter 3, the ALRC discusses the constitutional foundations of the *Privacy Act*, noting that the Act was passed on the basis of the Australian Parliament's express power to make laws with respect to 'external affairs'.[2] The external affairs power enables the Australian Parliament to make laws with respect to matters physically external to Australia;[3] and matters relating to Australia's obligations under bona fide international treaties or agreements, or customary international law.[4] The external affairs power is not confined to meeting international obligations, but may also extend to 'matters of international concern'.

8.5 The Preamble to the *Privacy Act* makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the United Nations *International Covenant on Civil and Political Rights* (ICCPR)[5] as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Guidelines).[6]

8.6 These international instruments are not expressed to apply to deceased individuals and, therefore, may not provide a firm constitutional basis for legislation at the federal level. It may be possible to argue that the limited provisions relating to

---

2 *Australian Constitution* s 51(xxix). See *Privacy Act 1988* (Cth) Preamble.

3 *Horta v Commonwealth* (1994) 181 CLR 183.

4 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Polyukhovich v Commonwealth* (1991) 172 CLR 501; *Horta v Commonwealth* (1994) 181 CLR 183.

5 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

6 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed further in Ch 1 and Part D.

deceased individuals recommended in this Report do fall within the rights protected by Article 17 of the ICCPR,[7] that they are matters of international concern,[8] or that they relate to the privacy rights of living individuals or are incidental to those rights. In order to avoid uncertainty, however, it may be preferable to seek a referral of power from the states under s 51(xxxvii) of the *Australian Constitution* in relation to the protection of the personal information of deceased individuals. Section 51(xxxvii) gives the Australian Parliament the power to make laws with respect to matters referred to the Parliament by the parliaments of the states.[9]

The *Privacy Act*

8.7 The *Privacy Act*, generally, does not protect the personal information of deceased individuals.[10] The term 'individual' is defined in the Act as 'a natural person'.[11] The Office of the Privacy Commissioner's (OPC) review of the private sector provisions of the *Privacy Act* (the OPC Review) stated that:

> The term 'natural person' is not defined under the *Privacy Act* or the *Acts Interpretation Act 1901*; however it appears the term is usually used to distinguish human beings from artificial persons or corporations. Whether the term 'natural persons' includes a deceased human being does not appear to have been subject to judicial consideration in Australia or the United Kingdom. The Office considers the term 'natural person' to mean a living human being as this is the plain English meaning of the term.[12]

8.8 The OPC, however, has suggested in guidance material issued in respect of the Information Privacy Principles (IPPs), that:

---

7 Art 17(1) provides that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. It could be argued, for example, that providing no protection for the personal information once individuals are deceased, impacts in an arbitrary way on the privacy of individuals while still alive. Individuals may be constrained in sharing information if they believe that information will be disclosed inappropriately when they die.

8 See the discussion of protecting the personal information of deceased individuals: European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP136 (2007), 22–23. See also, for example, the World Medical Association code of ethics, which provides that: 'A physician shall preserve absolute confidentiality on all he knows about his patient even after the patient has died': World Medical Association, *International Code of Medical Ethics* (2006) <www.wma.net/e/policy/c8.htm> at 18 April 2008.

9 Models to achieve national consistency in the regulation of privacy are discussed in Ch 3.

10 The exception is Part VIA of the *Privacy Act*, which deals with declared disasters and emergencies and is discussed further below and in detail in Ch 44.

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

12 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 281.

> Although information about dead people is not technically considered to be personal information, Agencies are encouraged to respect the sensitivities of family members when using or disclosing it.[13]

8.9 Part VIA of the *Privacy Act*—dealing with personal information in declared emergencies and disasters—explicitly states, however, that for the purposes of Part VIA, the definition of 'personal information' is 'taken to include a reference to an individual who is not living'. The provisions in Part VIA displace some of the requirements in the IPPs and National Privacy Principles (NPPs) by providing a separate regime for the collection, use and disclosure of personal information in the case of a declared emergency. The aim of Part VIA is to enhance information exchange between Australian Government agencies, state and territory authorities, organisations, non-government organisations and others, in emergencies and disasters. These provisions are discussed in more detail in Chapter 44.

8.10 The personal information of deceased individuals is expressly addressed in a range of other federal, state and territory legislation and receives some protection under the law relating to duties of confidentiality. The following section examines these laws and considers whether further protection is required.

Freedom of Information and Archives Acts

8.11 The *Freedom of Information Act 1982* (Cth) (the FOI Act) establishes a legally enforceable right of access to documents, including personal information, held by Australian Government public sector agencies. The Act sets out a number of exceptions to that right of access and these are described as 'exempt documents'. One class of exempt document is as follows:

> A document is an exempt document if its disclosure under this Act would involve the unreasonable disclosure of personal information about any person (including a deceased person).[14]

8.12 Where a request is made for access to the personal information of a deceased individual held by an agency and it appears to the decision maker under the FOI Act that the legal personal representative of the individual might reasonably wish to contend that the document should not be released, the representative must be given a reasonable opportunity to make submissions in relation to the matter.[15] Although the agency may consult under these provisions, the decision whether to release information remains with the agency. Where a decision is made that the personal information of a

---

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), 3.

14 *Freedom of Information Act 1982* (Cth) s 41(1). There are similar provisions in state and territory legislation. See, eg, *Freedom of Information Act 1989* (NSW) sch 1, pt 2 cl 6(1); *Freedom of Information Act 1982* (Vic) s 33(1); *Freedom of Information Act 1989* (ACT) s 41(1).

15 *Freedom of Information Act 1982* (Cth) s 27A. Legal personal representative includes the executor or administrator of a deceased individual's estate.

deceased individual is to be released under the FOI Act, the legal personal representative of the deceased person may apply to the Administrative Appeals Tribunal for review of the decision.[16] The FOI Act does not provide for amendment or annotation of personal information by a third party on behalf of a deceased individual.

8.13 When agencies no longer need ready access to records, most agencies are required to transfer them to the National Archives of Australia. The *Archives Act 1983* (Cth) deals with storage, disposal and destruction of such records. The Act also provides that, once records are 30 years old and in the open access period, they should be made available to the public, except in some circumstances. These include where they contain

> information or matter the disclosure of which under this Act would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person).[17]

8.14 Thus, while both the FOI Act and the *Archives Act* provide avenues for third parties to apply for access to information about deceased individuals, agencies are required to consider whether releasing the information would amount to an 'unreasonable disclosure'. These Acts are discussed in more detail in Chapter 15.

State and territory privacy legislation

8.15 New South Wales privacy and Victorian health privacy legislation covers personal information about individuals who have been dead for not more than 30 years.[18] This reflects the 30 year period after which government archival records are generally open to public access.[19] The Northern Territory *Information Act*, which combines privacy, freedom of information and archives provisions, covers personal information within the first five years after an individual dies.[20] Tasmanian privacy legislation extends protection to the personal information of individuals who have been dead for not more than 25 years,[21] and ACT health privacy legislation covers deceased individuals without imposing any time restrictions.[22]

8.16 Under the privacy principles and health privacy principles set out in these Acts, a number of situations arise in which a decision is required from an individual in relation to his or her personal information. For example, individuals are generally required to consent to the collection of sensitive information about them, such as their

---

16 Ibid s 59A.
17 *Archives Act 1983* (Cth) s 33(1)(g).
18 *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(a); *Health Records and Information Privacy Act 2002* (NSW) s 5(3)(a); *Health Records Act 2001* (Vic) ss 3(1), 95.
19 *Archives Act 1983* (Cth) s 3(7).
20 *Information Act 2002* (NT) s 4.
21 *Personal Information Protection Act 2004* (Tas) s 3.
22 *Health Records (Privacy and Access) Act 1997* (ACT) ss 4, 27 and dictionary (definition of 'consumer').

health information. In the case of a deceased individual, it is clearly impossible for the individual to make that decision or provide consent.

8.17 Instead, a number of these Acts include provisions that allow a decision to be made on behalf of the deceased individual. Under the *Health Records and Information Privacy Act 2002* (NSW), for example, an 'authorised representative' may make decisions on behalf of a deceased individual.[23] 'Authorised representative' includes 'a person who is otherwise empowered under law to exercise any functions as an agent of or in the best interests of the individual',[24] including an executor or administrator of a deceased estate. The arrangements established under these provisions extend to decisions on behalf of any individual that lacks capacity to make a decision under the Act, including deceased individuals.

Duty of confidentiality

8.18 A legal duty of confidentiality may arise in equity, at common law or under contract and provides some protection for personal information provided in confidence. How such duties arise and what they involve are discussed further in Chapters 15 and 16. A duty of confidence ends when the information loses its quality of confidence, whether through the passage of time, loss of secrecy or other change of circumstances.[25] This does not mean, however, that the duty necessarily ends when the person who has provided the information dies. The law of confidentiality, therefore, may provide some protection for the personal information of deceased individuals where that personal information was provided in confidence to, for example, banks, lawyers, doctors and others.

8.19 In a recent decision, the United Kingdom Information Tribunal found that health information relating to a deceased individual should not be released under the *Freedom of Information Act 2000* (UK) because a duty of confidentiality still existed. The Tribunal noted the argument put by one of the parties that, if individuals are aware that information they give to their health service providers may be disclosed to the public after their death, they may not make full disclosure, with the result that health service providers may be unable to provide appropriate medical treatment. The Tribunal agreed with this argument and expressed the view that:

> We believe that the public interest in maintaining confidentiality in the medical records of a deceased outweighs, by some way, the countervailing public interest in disclosure.[26]

---

23 *Health Records and Information Privacy Act 2002* (NSW) s 7.
24 Ibid s 8.
25 R Toulson and C Phipps, *Confidentiality* (2nd ed, 2006), 117.
26 *Bluck v Information Commissioner* [2007] UKIT EA 2006 0090, [13].

Genetic information

8.20 In the report *Essentially Yours: The Protection of Human Genetic Information* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC) recommended that:

> The Commonwealth should amend the *Privacy Act* to provide that 'health information' includes information about an individual who has been dead for 30 years or less. These amendments should include provision for decision making by next-of-kin or an authorised person in relation to the handling of a deceased individual's health information.[27]

8.21 Extending the protection of the *Privacy Act* to the genetic information of deceased individuals was justified on the basis of the implications this information may have for living genetic relatives.[28] The Australian Government noted in its response to ALRC 96 that this recommendation was being considered in the context of the development of the *National Health Privacy Code*.[29] The draft *National Health Privacy Code* was expressed to apply to the health information of individuals who have been dead for not more than 30 years.[30]

The OPC Review

8.22 The OPC Review noted that extending the *Privacy Act* to cover the personal information of deceased individuals would require some reworking of provisions and principles relating to consent and the lodging of complaints. The OPC Review recommended that this issue be considered in the context of a wider review of the Act.[31]

Issues Paper 31

8.23 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether the definition of 'personal information' in the *Privacy Act* should be amended to include the personal information of deceased individuals.[32]

---

27 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–6.

28 Ibid, [7.90].

29 Australian Government Attorney-General's Department, *Government Response to Australian Law Reform Commission and Australian Health Ethics Committee Report: Essentially Yours: The Protection of Human Genetic Information in Australia* (2005) <www.ag.gov.au> at 24 April 2008.

30 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4. The Code is discussed further in Ch 60.

31 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 85.

32 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 3–5.

Submissions and consultations

8.24 There was significant support expressed in submissions and consultations in response to IP 31 for extending at least some privacy principles to the personal information of deceased individuals.[33] Some of the problems arising from the handling of personal information of deceased individuals were highlighted in submissions. One individual noted that she was distressed by direct marketing companies attempting to contact her deceased husband.[34] Another expressed concern about an insurance company seeking to collect health information about him from his next of kin, in the mistaken belief that he was deceased.[35] One stakeholder provided a detailed case study of the difficulties encountered when her adopted sister died. A number of organisations refused to disclose her sister's personal information to her, or to allow insurance to be cancelled or accounts to be closed, even though she produced a death certificate and documents showing she was the administrator of her sister's estate. She stated:

> May I suggest, taking into account my personal and very distressing circumstances, that while appreciating a person's privacy needs to be protected, some common sense is applied in the case of a deceased person.[36]

8.25 In its submission, the Australian Privacy Foundation (APF) noted that there are good arguments both for and against extending privacy rights to cover the personal information of deceased individuals. The APF noted that not all the privacy principles sensibly apply to the personal information of deceased individuals. For example, the person cannot be notified or consulted about how his or her personal information is to be handled. The APF argued that it might be preferable to enact specific provisions to address this issue, rather than simply extend the definition of 'personal information' to include the personal information of deceased individuals.[37] A number of other stakeholders also expressed the view that the principles should apply only so far as is practicable.[38]

---

33 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; 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; Australian Institute of Health and Welfare, *Submission PR 170*, 5 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

34 A Baxter, *Submission PR 74*, 5 January 2007.

35 Confidential, *Submission PR 223*, 8 March 2007.

36 N Sertori, *Submission PR 349*, 23 November 2007.

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

38 National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007.

8.26 AAMI expressed support for extending the *Privacy Act* to cover the information of deceased individuals:

> AAMI often sadly is dealing with a deceased person's information, mainly as a result of a fatality claim on a motor vehicle insurance policy or as part of a compulsory third party (CTP) claim. AAMI currently applies its privacy protection procedures to the deceased personal information as it would to a natural person, as far as is practicable. Therefore AAMI supports amending the Act to include personal information of the deceased, with the provision that in certain circumstances it may not be practicable.[39]

8.27 Other organisations noted that, to simplify matters, or in order to comply with state and territory legislation, as far as possible they handle the personal information of deceased individuals in the same way as they handle the personal information of living individuals.[40] The Australian Government Department of Community Services expressed support for extending the *Privacy Act* to cover the personal information of deceased individuals and noted that the secrecy provisions included in Medicare and Centrelink legislation continued to cover individuals after death.[41]

8.28 The Centre for Law and Genetics expressed support for extending the *Privacy Act* to cover the personal information of deceased individuals and noted that the justification is particularly strong in relation to Indigenous communities. It noted that those communities have 'religious and spiritual concerns about representations of deceased individuals'.[42]

8.29 The NHMRC stated that:

> The present situation, whereby the health information of deceased persons is protected by legislation in several States and Territories but not by Commonwealth legislation adds to the complexity and confusion created by the existing regulatory regime; and
>
> Information about the health of deceased persons, in particular but not limited to genetic information, may have significant implications for living relatives, both genetic and non-genetic. It is preferable for representatives of the deceased to be able to consent to collection, use and disclosure of such information.[43]

8.30 Some concerns were raised about extending the *Privacy Act* to include the personal information of deceased individuals. These included: increased complexity for executors, family members and insurance companies following the death of an individual;[44] more limited access to information for research and other activities of

---

39 AAMI, *Submission PR 147*, 29 January 2007.

40 National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007.

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

42 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007. See also the discussion of the particular privacy needs of Indigenous people in Ch 7.

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

44 Australian Health Insurance Association, *Submission PR 161*, 31 January 2007.

interest to family members or in the public interest;[45] and an additional compliance burden for business.[46]

8.31 The Australian Federal Police did not support extending the *Privacy Act* to cover the personal information of deceased individuals because of the potential to complicate their investigations relating to such persons.[47] The Australian Tax Office stated that:

> In our view, there may be some justification for expanding the definition to include information about the deceased, particularly health and medical information. However, we would be hesitant to recommend any changes that would restrict the way that regulatory and enforcement agencies can access information about the deceased to maintain up-to-date and accurate registers. The ability to collect and use information about deceased persons helps us to keep our taxpayer records as accurate as possible. Access to this information is also a key way of combating identity fraud as it helps to prevent 'new' identities being registered using details of the deceased.[48]

8.32 A number of stakeholders also commented on the difficulties that arise when it is necessary to seek decisions on behalf of deceased individuals from alternative decision makers. One stakeholder noted that family members often do not speak with one voice on such matters.[49] Other stakeholders noted that obtaining consent can be difficult, especially where there is a dispute in the family,[50] and that it becomes more difficult to identify and locate alternative decision makers as time passes.[51] Where it is not possible to identify and locate an alternative decision maker, this may mean that information cannot be collected, used or disclosed.

8.33 The State Records Office of Western Australia commented that concerns about sensitive personal information of deceased individuals tend to diminish over time.[52] The Privacy Committee of South Australia noted that, in dealing with the personal information of deceased individuals, it was necessary to balance privacy concerns with what is reasonable and what is in the public interest.[53]

Discussion Paper proposals

A new part in the *Privacy Act*

8.34 In DP 72, the ALRC expressed the preliminary view that simply amending the definition of 'personal information' to include the personal information of deceased

---

45 Government of South Australia, *Submission PR 187*, 12 February 2007; Australian Institute of Health and Welfare, *Submission PR 170*, 5 February 2007; Public Record Office Victoria, *Submission PR 72*, 3 January 2007.

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

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

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

49 Public Record Office Victoria, *Submission PR 72*, 3 January 2007.

50 Banking and Financial Services Ombudsman, *Consultation PC 76*, Melbourne, 5 February 2007.

51 B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007.

52 State Records Office of Western Australia, *Consultation PC 67*, Perth, 24 January 2007.

53 Privacy Committee of South Australia, *Consultation PC 110*, Adelaide, 1 March 2007.

individuals would be problematic. In particular, many of the privacy principles could not apply at all, or could apply only in part, to such information. It appeared more appropriate and workable to indicate the extent to which the privacy principles would apply.

8.35 The ALRC proposed that the *Privacy Act* should be amended to include a new part dealing with the personal information of deceased individuals who had been dead for 30 years or less.[54] The proposed new part was to include provisions on use and disclosure, access, data quality, data security, genetic information and complaints. Each of these proposed provisions is discussed in more detail below. The part was only to apply to organisations. The ALRC proposed that the personal information of deceased individuals held by agencies should continue to be regulated by the FOI Act and the *Archives Act*.

Submissions and consultations

8.36 In response to the ALRC's proposal, a number stakeholders expressed the view that the *Privacy Act* should not be extended to cover the personal information of deceased individuals.[55] The Law Council of Australia stated that:

> The common law operates such that actions in personam, including, for example, defamation, should not extend to the deceased. This is because a person's relevant interests do not continue after they have died. Similar to defamation law, the laws relating to privacy are designed to prevent hurt, humiliation and other such injuries to feelings, rather than to protect a property right. Necessarily, and unlike a property right, the ability to experience the feelings with which privacy law is concerned passes with death. Privacy rights, and the remedies they provide, cannot therefore assist deceased people, and should not apply after death.[56]

8.37 The Australian Direct Marketing Association noted that it is often difficult for organisations to know whether an individual is deceased.[57] Axciom Australia suggested that introducing a right of access to the personal information of deceased individuals would give rise to confusion, given the current privacy regime is based around access by an individual to his or her own information.[58] The Australian Government Department of Agriculture, Fisheries and Forestry noted that the provisions may give rise to particular issues for Indigenous people, given cultural concerns associated with information about deceased individuals.[59]

---

54 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–11.

55 GE Money Australia, *Submission PR 537*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Australian Library and Information Association, *Submission PR 446*, 10 December 2007.

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

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

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

59 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

8.38 The Public Interest Advocacy Centre (PIAC) was concerned that the proposed provisions would 'place unjustified constraints on legitimate social and historical research, which is often in the public interest'.[60] The School of Public Health at the University of Sydney argued that the proposed provisions should not inhibit the use of the personal information of deceased individuals for research purposes, with appropriate safeguards.[61] In the OPC's view, the provisions should be limited to the health information of deceased individuals.[62]

8.39 On the other hand, a number of stakeholders expressed support for the ALRC's proposals.[63] The NHMRC noted, however, that guidance from the Privacy Commissioner may be required in some areas.[64]

8.40 The Office of the Victorian Privacy Commissioner (OVPC) suggested that the protection of personal information is comparable to duties of confidentiality. Unlike a right to sue for defamation, duties of confidentiality can persist after death. The OVPC stated that, without such protection, individuals may be less inclined to share information, particularly sensitive information, through concern that it might be used or disclosed inappropriately when they die.[65]

8.41 The Law Society of New South Wales supported the proposals, but suggested that the provisions should require those wishing to use or disclose such information to take reasonable steps to determine the wishes of the deceased individual, as evidenced in a will or other document.[66]

8.42 In supporting the proposal, the Australian Bankers Association (ABA) stated that, as far as possible, banks handle the personal information of deceased individuals in much the same way as they handle the personal information of living individuals. In the ABA's view, the personal information of both should be regulated in the same way.[67] The ABA and the National Australia Bank stressed that the proposed provisions should not impose a requirement to retain records for a period of 30 years. They noted that, generally, organisations are only required to retain records for seven years.[68]

---

60 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
61 School of Public Health—University of Sydney, *Submission PR 504*, 20 December 2007.
62 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
63 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.
64 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007. National Legal Aid agreed that guidance would be necessary: National Legal Aid, *Submission PR 521*, 21 December 2007.
65 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
66 Law Society of New South Wales, *Submission PR 443*, 10 December 2007.
67 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.
68 Ibid; National Australia Bank, *Submission PR 408*, 7 December 2007.

ALRC's view

8.43 The ALRC has considered stakeholder views on extending the *Privacy Act* to cover the personal information of deceased individuals. Those views were varied and fairly evenly distributed between those who supported the ALRC's proposals and those who did not. On balance, in the ALRC's view, the *Privacy Act* should be amended to include provisions on the handling of personal information of deceased individuals where that information is held by organisations. This would have a number of benefits. It would introduce a level of consistency in the way this information is handled across the private sector. Currently, personal information held by organisations may be subject to state or territory legislative requirements, a duty of confidentiality or simply dealt with as a matter of organisational policy. It would also allow the Privacy Commissioner to become involved where there is a dispute about the handling of such information.

8.44 The ALRC notes the view that the right to privacy attaches to the individual and should not survive the death of the individual, but is of the view that there are legitimate public policy reasons for extending some protection to the personal information of deceased individuals. These include: the fact that individuals may hesitate to share personal information while they are alive if they believe that the information may be handled inappropriately after they die; the need for living individuals to access the personal information of deceased individuals in some circumstances; and the distress caused to living individuals where the personal information of deceased individuals is handled inappropriately. The ALRC notes that these issues are not confined to the handling of the health information of deceased individuals and so has not confined its recommendations to health information, as suggested by the OPC.

8.45 The ALRC has considered the concern that it can be difficult to know whether an individual is deceased. NPP 3 currently requires organisations to take reasonable steps to ensure that personal information they collect, use or disclose is accurate, complete and up-to-date.[69] In many situations, the inquiries necessary to meet this requirement will indicate whether the individual is living or deceased. Other situations, for example, requests for access to the personal information of deceased individuals made by third parties, will provide the opportunity for organisations to confirm whether an individual is living or deceased. It may be, for example, that the third party is asked to provide evidence that the individual is deceased before the organisation releases any information.

8.46 In the ALRC's view, it is not practicable simply to extend the definition of 'personal information' in the *Privacy Act* to include the personal information of deceased individuals. It is clear that not all of the current privacy principles, or indeed

---

69 These criteria are retained in the 'Data Quality' principle in the model UPPs.

all of the model UPPs, can be applied sensibly, or applied in full, to the personal information of deceased individuals. The 'Notification' principle, for example, would have no application. Instead, the *Privacy Act* should be amended to include specific provisions for the use and disclosure, data quality and data security of the personal information of deceased individuals, and to provide a right of access to such information.

8.47 The *Privacy Act* also should be amended to include a new part dealing with information about individuals who have been dead for 30 years or less. This does not mean that organisations will be required to keep information for 30 years if not otherwise required to do so. Organisations will be required to handle information in accordance with the recommended provisions for a period of 30 years following the death of the individual. It may be that information can be destroyed before the expiry of the 30 year period in accordance with the data security provision, discussed below.

Agencies

8.48 In DP 72, the ALRC proposed that the personal information of deceased individuals held by agencies should continue to be regulated by the FOI Act and the *Archives Act*.[70]

Submissions and consultations

8.49 A number of stakeholders expressed support for this proposal.[71] The Government of South Australia supported the proposed provisions on the basis that 'they leave responsibility for access to State and Territory public sector information to the relevant State and Territory laws'.[72]

8.50 Other stakeholders noted, however, that this would introduce a level of inconsistency into the proposed regime and were of the view that the new provisions of the *Privacy Act* relating to deceased individuals should apply to both agencies and organisations.[73] Privacy NSW was also of the view that agencies should be covered, to the extent that the provisions were not inconsistent with the FOI Act. It argued that elements of the proposed regime, such as the data quality and data security provisions—which do not have equivalents in the FOI Act—should apply to the personal information of deceased individuals held by agencies.[74]

---

70 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–10.

71 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 Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

73 Confidential, *Submission PR 570*, 13 February 2008; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

ALRC's view

8.51 While acknowledging stakeholder concerns about inconsistency between agencies and organisations, the ALRC has come to the view that the existing regime for dealing with the personal information of deceased individuals held by agencies under the FOI Act and the *Archives Act* should remain in place. The archiving and destruction of personal information of deceased individuals held by agencies should continue to be regulated by the *Archives Act.* At the state and territory level, access to personal information of deceased individuals held by public sector agencies should continue to be regulated by state and territory legislation.

8.52 In Chapter 29, the ALRC recommends that the 'Access and Correction' principle apply to both agencies and organisations.[75] The principle, reflecting the overall focus of privacy legislation, is limited to access and correction of an individual's own personal information. In the ALRC's view, it is appropriate that access and correction of one's own information be dealt with primarily under the *Privacy Act.*

8.53 The situation is not as clear cut in relation to the personal information of deceased individuals. Access to the personal information of a deceased individual involves access to the personal information of a third party. This is not the primary focus of the *Privacy Act*. The handling of information held by agencies about third parties—whether living or deceased—is currently governed by the FOI Act and the *Archives Act*. These Acts provide a framework within which such information may be disclosed, archived or destroyed and provide individuals with a right of access to such information in appropriate circumstances. While it is possible to argue that the use and disclosure of, and access to, the personal information of deceased individuals held by agencies could be regulated under the *Privacy Act*, on balance, the ALRC recommends no change to these arrangements. In DP 72, the ALRC proposed that the personal information of deceased individuals held by agencies should continue to be regulated by the FOI Act and the *Archives Act*. This has not been included as a recommendation in this Report as no change to the existing arrangements is required.

8.54 Given the issues raised by stakeholders, however, the ALRC recommends a number of limited provisions, to be included in the *Privacy Act*, specifically regulating the personal information of deceased individuals held by organisations. Each of these provisions is discussed in detail below.

Use and disclosure

8.55 In DP 72, the ALRC proposed that organisations should be required to use or disclose the personal information of deceased individuals in accordance with the 'Use

75 Rec 29–1.

and Disclosure' principle in the UPPs. Where the principle required consent, the ALRC proposed that the organisation be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.[76] This test mirrors the requirement imposed on agencies under the FOI Act, in considering whether to provide access to information about third parties.[77]

Submissions and consultations

8.56 A number of organisations noted that, in the course of finalising and administering the estates of a deceased individual—including insurance and superannuation policies—it is necessary to contact third parties such as employers, relatives and friends and to disclose the personal information of the deceased individual to such parties. These organisations wished to ensure that the proposed regime would allow this to continue.[78]

8.57 The National Australia Bank stated that:

> NAB appreciates the rationale for the extension of the privacy regime to deceased persons. From a practical implementation perspective, NAB's preliminary view would be that it may be an 'unreasonable use or disclosure' of a deceased person's information or would have 'unreasonable impact' on the privacy of a deceased individual, unless the information was disclosed to a person who was able to provide documented evidence of their entitlement to the information, for example, next of kin or a legal representative.[79]

8.58 PIAC suggested that, in relation to use and disclosure, the test should be whether it would involve an unreasonable use or disclosure of the personal information of any *living* individual. PIAC did not support asking organisations to decide whether a proposed use or disclosure involved an unreasonable use or disclosure of the personal information of deceased individuals. In PIAC's view, privacy is an individual right and, once individuals are deceased, they cannot be harmed in any way by the use or disclosure of their personal information.[80]

8.59 The OPC was of the view that the 'unreasonable use or disclosure' test was problematic and would create uncertainty. In addition, the OPC argued that disclosure should only be available to those with a legitimate interest in the information. The OPC suggested that this be limited by reference to the definition of 'responsible person' in

---

76 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–11.
77 *Freedom of Information Act 1982* (Cth) s 41.
78 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; AXA, *Submission PR 442*, 10 December 2007.
79 National Australia Bank, *Submission PR 408*, 7 December 2007.
80 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

NPP 2.5, which includes parents, adult children, siblings and other relatives, spouses, and de facto spouses.[81]

ALRC's view

8.60 The *Privacy Act* should be amended to provide that organisations must use or disclose the personal information of deceased individuals in accordance with the 'Use and Disclosure' principle. An organisation should be allowed to use or disclose such information, for example, where the information is being used or disclosed for the primary purpose of collection; or a secondary purpose that is related to (in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the agency or organisation to use or disclose the information for that purpose. This would include, for example, using and disclosing the personal information of a deceased individual in the course of administering his or her life insurance policy or superannuation policy.

8.61 Under the 'Use and Disclosure' principle, it would also be possible to use or disclose the personal information of deceased individuals, for example, as part of an investigation into suspected unlawful activity;[82] where required or authorised by or under law;[83] or for research.[84]

8.62 Where a use or disclosure under the principle would require consent, however, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. The ALRC does not agree that this consideration should be limited to whether the proposed use or disclosure would involve an unreasonable use or disclosure of the personal information of living individuals. It would be important to consider, for example, whether the use or disclosure would be unreasonable given the cultural sensitivities or expressed wishes of the deceased individual.

8.63 An organisation should be permitted to use or disclose the information without consent, however, where it is reasonable to do so in all the circumstances. This is consistent with the test imposed on agencies under the FOI Act relating to the release of information in response to an access request. The test of what amounts to 'unreasonable disclosure' has been considered in the FOI context:

---

81 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
82 UPP 5.1(d).
83 UPP 5.1(e).
84 UPP 5.1(g).

> The application of the test involves a consideration of all the factors relevant in a particular case and a balancing of all legitimate interests (*Wiseman v. Commonwealth*, (D251) eg *Re Chandra and Minister for Immigration and Ethnic Affairs* (D33)).[85]

8.64 There are circumstances in which it would be reasonable for organisations to use or disclose the personal information of deceased individuals for a secondary purpose unrelated to the primary purpose of collection, for example, in response to a request from a family member undertaking family history research. In considering all the factors relevant to a particular case and balancing all legitimate interests, organisations will need to consider issues such as any existing duty of confidentiality to the deceased individual, the interests of other family members and any public interest in the use or disclosure. In some circumstances it may be important to contact family members or the deceased individual's legal personal representative, or to consider the terms of the deceased individual's will, in order to be able to make an informed decision about what is reasonable.

8.65 This same test should be applied to the use or disclosure of sensitive information.[86] In considering what is reasonable, the organisation would be required to consider the sensitivity of the information.

Access

8.66 In DP 72, the ALRC proposed that organisations should be required to consider providing third parties with access to the personal information of deceased individuals in accordance with the access elements of the 'Access and Correction' principle. The ALRC suggested that organisations should be required to consider in each case whether providing access to the information would have an unreasonable impact on the privacy of other individuals, including the deceased individual.[87] This test mirrors one of the current exemptions in NPP 6.1(c) on access and correction.

8.67 The ALRC also expressed the view that a third party should not have a right to seek to correct the personal information of a deceased individual under the *Privacy Act*. This is consistent with the position under the FOI Act. In relation to the personal information of deceased individuals, the data quality provision, recommended below, will operate to ensure that information is kept accurate, complete, up-to-date and relevant. In order to comply with the data quality provision, organisations would need to consider information provided by third parties relating to the personal information of a deceased individual.

---

85 Australian Government Attorney-General's Department, *Freedom of Information Memorandum 98: Exemption Sections in the FOI Act* (2005).

86 Health information of deceased individuals is discussed further below.

87 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–11.

Submissions and consultations

8.68 While the OPC supported a limited discretion to disclose the health information of deceased individuals, the OPC did not support creating a right of access to the personal information of deceased individuals. The OPC stated that:

> 'Access' is constructed under the *Privacy Act* to create a positive right for individuals to know what information is held about them by organisations and agencies. Organisations and agencies may only deny it where such denial is specifically permitted by prescribed exceptions. This can be contrasted, for example, with the 'use and disclosure' principle which creates discretions for parties to use or disclose the information. Accordingly, the provision of a deceased person's information to a third party appears to sit more comfortably as an example of a 'disclosure', rather than the provision of 'access'. Further, the Office submits that the mechanism should be discretionary and, therefore, fit neatly as an exception to the 'disclosure' principle.[88]

8.69 On the other hand, PIAC was of the view that there were circumstances in which third parties have legitimate grounds to seek access to the personal information of a deceased individual and that organisations should be required to consider providing such access.

> For example, members of the Aboriginal 'Stolen Generation' need to be able to obtain information about deceased relatives in order to find their identity and re-establish family and community links.[89]

8.70 The Human Rights and Equal Opportunity Commission (HREOC) also expressed support for allowing a right of access to the personal information of deceased individuals in some circumstances.[90] HREOC highlighted the following passage from *Bringing Them Home*, the report of the National Inquiry into the separation of Aboriginal and Torres Strait Islander children from their families:

> The need to protect one person's privacy has to be weighed against the need to provide another with access to personal information. The refusal to release third party identifying information could deny an Indigenous searcher the opportunity for reunion with his or her family and/or community and access to entitlements for which proof of community connection or Aboriginality generally is required.[91]

8.71 A number of stakeholders expressed the view that it would be difficult to assess which third parties should have access to a deceased individual's information.[92] The Financial Planning Association of Australia noted that:

---

88 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
89 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
90 Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007.
91 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), 350.
92 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007.

> Where there are complex family connections … it may be difficult to determine the relationship and, in some circumstances, it may be inappropriate to provide information. In such cases we would suggest that financial planners should not have an obligation to provide sensitive information to anyone other than the executor of the estate.[93]

8.72 The Insurance Council of Australia suggested that individuals requiring access to personal information of deceased individuals should be required to establish a reasonable connection with the deceased individual and a legitimate reason for requesting access to the information.[94] ANZ stated that the right of access to financial information should be limited to those with legal rights to administer the estate of the deceased individual.[95] The Avant Mutual Group Ltd expressed the view that the right of access to health information should be limited to those with legal rights to administer the estate of the deceased individual and immediate family members with a legitimate need for access to the information.[96]

ALRC's view

8.73 The ALRC has carefully considered the OPC's view that the *Privacy Act* should be amended to allow for discretionary disclosure of deceased individuals' information, but should not include a right of access to such information. In the ALRC's view, however, it is important to provide a right of access to the personal information of deceased individuals for a number of reasons. The first is that, in some circumstances, it is crucial for individuals to be able to access the personal information of deceased individuals, for example, to understand their genetic health risks or to trace their family history. In such cases, in the ALRC's view, more than a discretion to disclose is required. There should be a right to access such information.[97]

8.74 Secondly, it is important to ensure that individuals seeking access to the personal information of deceased individuals have recourse to the conciliation and determination processes under the *Privacy Act*. It is unclear from the OPC's submission on what basis an individual would complain to the Privacy Commissioner if an organisation exercised its discretion not to disclose information. Providing a right of access to information provides a clear basis for individuals seeking access to information to have recourse to Privacy Commissioner if access is denied.

---

93 Financial Planning Association of Australia, *Submission PR 496*, 19 December 2007.

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

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

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

97 In ALRC 96, the ALRC and the Australian Health Ethics Committee (AHEC) recommended that the *Privacy Act* be amended to provide that an individual has a right to access genetic information about first-degree genetic relatives where such access is necessary to lessen or prevent a serious threat to the individual's life, health, or safety. See Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 21–3.

8.75 Organisations should be required to provide third parties with access to the personal information of deceased individuals in accordance with the access elements of the 'Access and Correction' principle, except to the extent that providing access to the information would have an unreasonable impact on the privacy of other individuals, including the deceased individual. In considering the impact on the privacy of the deceased individual, an organisation might consider, for example, the sensitivity of the information and any expressed wishes of the individual. In deciding what is reasonable, organisations will be required to consider all the circumstances, including the relationship of the individual requesting access to the deceased individual.

8.76 All the other exceptions in the 'Access and Correction' principle would apply. For example, an organisation would not be required to provide access to the information if denying access was required or authorised by or under law. This would include situations in which information was protected by a duty of confidentiality, discussed above.

Data quality

8.77 In DP 72, the ALRC proposed that organisations should be required to ensure that the personal information of deceased individuals is, with reference to a use or disclosure permitted under the model UPPs, accurate, complete, up-to-date and relevant before they use or disclose the information.[98]

Submissions and consultations

8.78 One stakeholder suggested that organisations should be required to take 'reasonable steps' to ensure that the personal information of deceased individuals is accurate, complete, up-to-date and relevant before they use or disclose the information.[99] PIAC noted that it may be difficult to check data quality in relation to the personal information of deceased individuals without contacting living relatives or legal representatives, and that the information is likely to lose currency after the individual's death.[100]

8.79 The OPC agreed:

> The Office notes that the current NPP on data quality requires that an organisation take 'reasonable steps' to make sure that information it is about to use is accurate, complete and up-to-date. The Office suggests that consideration should be given to the inclusion of this term in [the 'Data Quality' provision].[101]

98 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–11(c).
99 Confidential, *Submission PR 519*, 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.

ALRC's view

8.80 The ALRC agrees that organisations should be required to take 'reasonable steps' to ensure that the personal information of deceased individuals is accurate, complete, up-to-date and relevant before they use or disclose the information. This is consistent with the language of the 'Data Quality' principle. The ALRC recommends, therefore, that organisations should be required to comply with the use and disclosure elements of the 'Data Quality' principle in relation to the personal information of deceased individuals.[102]

Data security

8.81 In DP 72, the ALRC proposed that organisations should be required to take reasonable steps to: protect the personal information of deceased individuals from misuse and loss and from unauthorised access, modification or disclosure; and destroy or render personal information of deceased individuals non-identifiable if it is no longer needed for any purpose permitted under the model UPPs.[103]

Submissions and consultations

8.82 In response, PIAC and HREOC expressed concern about the requirement that the personal information of deceased individuals be destroyed in some circumstances, noting the potential adverse impact on social and medical research, and the ability of Indigenous individuals to identify their families and communities.[104] PIAC also discussed the importance of protecting personal information from destruction in the context of investigating claims that Indigenous individuals were denied access to wages, allowances and pensions held on trust by the Aborigines Welfare Board and the New South Wales Government (the 'Stolen Wages Project'). PIAC noted that

> the destruction of or inability to locate the records of private organisations that were involved in the custody and employment of Indigenous people has created and remains a significant barrier to some claimants.[105]

ALRC's view

8.83 In Chapter 28, the ALRC discusses the 'Data Security' principle in detail, including the requirement to destroy or render non-identifiable personal information that is no longer needed for any purpose permitted by the UPPs. In that chapter, the ALRC discusses the retention of information where it may be needed for the purposes of litigation, dispute resolution and research. The ALRC recommends that the 'Data Security' principle, as proposed in DP 72, be amended to require that agencies and

---

102 The 'Data Quality' principle also applies to the collection of personal information relating to living individuals, but the ALRC does not recommend that this element of the principle be applied to the personal information of deceased individuals.

103 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–11(d).

104 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500,* 20 December 2007.

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

organisations take reasonable steps 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 where retention is not required or authorised by or under law.[106] The ALRC also recommends that the OPC develop and publish guidance on these issues. This should include guidance on dealing with information that forms part of a historical record or may need to be preserved for the purpose of future dispute resolution.[107]

8.84 On the basis of these recommendations, in the ALRC's view, organisations should be required to comply with the 'Data Security' principle in relation to the personal information of deceased individuals.

Contractors

8.85 In DP 72, the ALRC proposed that organisations be required to take reasonable steps to ensure that personal information of deceased individuals disclosed pursuant to contract, or otherwise in connection with the provision of a service, is protected from being used or disclosed otherwise than in accordance with the *Privacy Act*.[108] This requirement reflected one element of the 'Data Security' principle proposed in DP 72.[109]

ALRC's view

8.86 In Chapter 28, the ALRC notes that this element of the 'Data Security' principle will not be necessary if the recommendations in this Report are implemented. The provision was intended to address the situation in which information handling is contracted out, in particular to small businesses not covered by the *Privacy Act*. Once the recommendations in this Report are implemented, however, there will be no need to cover this regulatory 'gap' as agencies and organisations, including organisations that are small businesses, will be covered by the model UPPs. On this basis, the ALRC is of the view that this element is not required in the data security provisions applicable to the personal information of deceased individuals.

Recommendation 8–1 The *Privacy Act* should be amended to include provisions dealing with the personal information of individuals who have been dead for 30 years or less where the information is held by an organisation. The Act should provide as follows:

(a) Use and Disclosure

106 Rec 28–4.
107 Rec 28–5.
108 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–11.
109 Ibid, Proposal 25–2.

Organisations should be required to comply with the 'Use and Disclosure' principle in relation to the personal information of deceased individuals. Where the principle would have required consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. The organisation must not use or disclose the information if the use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

(b) Access

Organisations should be required to provide third parties with access to the personal information of deceased individuals in accordance with the access elements of the 'Access and Correction' principle, except to the extent that providing access would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

(c) Data Quality

Organisations should be required to comply with the use and disclosure elements of the 'Data Quality' principle in relation to the personal information of deceased individuals.

(d) Data Security

Organisations should be required to comply with the 'Data Security' principle in relation to the personal information of deceased individuals.

Genetic information

8.87 In ALRC 96, the ALRC and AHEC recommended that:

- the *Privacy Act* should be amended to permit the disclosure of an individual's genetic information to a genetic relative where the disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety;[110]

- the *Privacy Act* should be amended to provide individuals with a right to access genetic information about first-degree genetic relatives where such access is necessary to lessen or prevent a serious threat to the individual's life, health, or

110 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 21–1.

safety. The right of access could be refused where providing access would have an unreasonable impact upon the privacy of any individual;[111] and

- the NHMRC, in consultation with the OPC, should develop guidelines dealing with the disclosure of, and access to, genetic information in these circumstances.[112]

8.88 The *Privacy Act* was subsequently amended to implement two of these three recommendations. The new provision, NPP 2.1(ea), allows an organisation to use or disclose an individual's genetic information where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative of the individual. NPP 2.1(ea) also provides that any such use or disclosure must be in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner. The *Privacy Act* was not, however, amended to implement Recommendation 21–3, in relation to providing a right of access to genetic information.

8.89 In Chapter 63, the ALRC considers NPP 2.1(ea) and recommends that the provision be moved to the new *Privacy (Health Information) Regulations*. The ALRC also recommends that the provision be amended to apply to both agencies and organisations and that the reference to guidelines issued by the NHMRC be replaced with a reference to rules issued by the Privacy Commissioner. It is anticipated that these rules will address issues such as providing genetic information through a nominated medical practitioner or genetic counsellor, who can explain the clinical relevance of the information.[113]

8.90 In DP 72, the ALRC proposed that the provisions dealing with the use or disclosure of personal information of deceased individuals should make clear that it is reasonable for an organisation to use or disclose genetic information to a genetic relative of a deceased individual where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative.[114]

111 Ibid, Rec 21–3.
112 Ibid, Rec 21–2.
113 Rec 63–5.
114 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–12.

Submissions and consultations

8.91 A number of stakeholders expressed support for the ALRC's proposal concerning the release of genetic information of a deceased individual to a genetic relative.[115]

8.92 The OPC suggested that the intent of the proposal could be achieved more simply by extending the application of existing NPP 2.1(ea) to include the genetic information of deceased individuals.[116]

ALRC's view

8.93 The ALRC agrees that NPP 2.1(ea)—to be moved to the new *Privacy (Health Information) Regulations* in accordance with Recommendation 63–5—should be extended to apply to the use and disclosure of genetic information of deceased individuals to their genetic relatives. This will ensure that any such use and disclosure is conducted in accordance with the rules to be issued by the Privacy Commissioner.

8.94 Recommendation 21–3 of ALRC 96—providing a right of access to the genetic information of a genetic relative—should be implemented and should, as recommended in ALRC 96, extend to the personal information of deceased individuals. In ALRC 96, the ALRC and AHEC recommended that any such access should be provided in accordance with binding guidelines to be issued by the NHMRC and approved by the Privacy Commissioner. In order to be consistent with other recommendations in this Report,[117] those guidelines should be renamed rules and should be issued by the Privacy Commissioner.

Recommendation 8–2 The *Privacy Act* should be amended to provide that the content of National Privacy Principle 2.1(ea) on the use and disclosure of genetic information to genetic relatives—to be moved to the new *Privacy (Health Information) Regulations* in accordance with Recommendation 63–5—should apply to the use and disclosure of genetic information of deceased individuals.

Consultation with and decisions by third parties

8.95 As discussed above, some state and territory privacy legislation makes provision for decisions to be made by third parties on behalf of deceased individuals where a decision is required in relation to the deceased individual's personal information.

---

115 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

117 Recs 47–2 and 63–5.

8.96 In addition, under the FOI Act where there is a request to access the personal information of a deceased individual, the Act requires agencies, in some circumstances, to provide a deceased individual's legal personal representative with a reasonable opportunity to make submissions in relation to the request.[118] The agency, however, retains the power to make the decision on whether access is granted.[119]

8.97 In ALRC 96, the ALRC and AHEC recommended that the definition of 'health information' in the *Privacy Act* be amended to include information about an individual who has been dead for 30 years or less and that these amendments should include provision for decision making by next-of-kin or an authorised person.[120] In ALRC 96, the ALRC and AHEC noted, however, that:

> If the law requires that access to genetic information about a deceased individual can be granted only with the consent of that person's legal or other authorised representative, genetic relatives may still have problems in gaining access.[121]

ALRC's view

8.98 In considering whether to impose an obligation on organisations to consult with third parties, or a requirement to seek a decision from a third party on behalf of a deceased individual, the ALRC considered the difficulties with these processes highlighted by stakeholders. These included: the fact that family members and other third party representatives often have different views on the appropriateness of access to information, or the sensitivity of that information; the difficulties in finding and contacting relevant third parties; and the fact that this becomes more difficult over time. In relation to requests for access to health information, genetic information or family history information, in particular, the ALRC's view is that one individual or family member should not be able to stop another family member from gaining access to a deceased family member's information. For this reason the ALRC is no longer of the view, expressed in ALRC 96, that provision should be made for decision making by next-of-kin or another authorised person.

8.99 The ALRC also considered the likely compliance costs such processes would impose on organisations. On balance, the ALRC considers that such an obligation or requirement should not be imposed on organisations.

8.100 Instead, where a decision by the individual would have been required, the ALRC recommends that organisations dealing with the personal information of a deceased individual be required to decide whether the proposed use or disclosure would involve 'an unreasonable use or disclosure of personal information' or whether

---

118 *Freedom of Information Act 1982* (Cth) s 27A.
119 Ibid s 41.
120 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–6.
121 Ibid, [7.93].

providing access to the information would have 'an unreasonable impact on the privacy of other individuals, including the deceased individual'.

8.101 The decision to use or disclose, or to provide access to, the information should remain with the organisation, rather than with a third party representing the deceased individual. In order to make informed decisions in this area, organisations may find it useful, or even necessary, to consult deceased individuals' families or legal personal representatives but the ALRC does not propose that there be a legal requirement to do so in the *Privacy Act.*

Complaints

8.102 In DP 72, the ALRC proposed that breach of the provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. This would allow a complaint to be lodged with the Privacy Commissioner. The ALRC's preliminary view was that the following individuals should have standing to lodge a complaint:

- in relation to an alleged breach of the use and disclosure, data quality or data security provisions—the deceased individual's parent, child or sibling who is at least 18 years old, spouse, de facto partner or legal personal representative; and

- in relation to an alleged breach of the access provision—any person who has made a request for access to the personal information of a deceased individual.[122]

Submissions and consultations

8.103 A number of stakeholders expressed support for the ALRC's proposal in relation to standing to make complaints.[123] The OVPC suggested that the categories of people with standing should be expanded to include 'any other individual who, in the opinion of the Privacy Commissioner, has a sufficient interest in the subject-matter of the complaint'.[124]

8.104 The OPC agreed that parents, children, siblings, spouses, de facto partners or legal personal representatives should have standing to lodge a complaint alleging an interference with the privacy of a deceased individual. The OPC did have concerns, however, about denial of access giving rise to a complaint:

> The Office submits that, in many cases, it may be inappropriate to consider a denial of 'access' to a deceased individual's information as an interference with the privacy of the deceased. This is particularly the case, for example, if the interests of the

122 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 3–13.
123 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; P Youngman, *Submission PR 394*, 7 December 2007.
124 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. See *Information Privacy Act 2000* (Vic) s 27.

> requesting party are commercial rather than personal. Such a construction may not align with a general understanding of what an interference with privacy may entail.[125]

8.105 PIAC, and one other stakeholder,[126] expressed the view that only third parties whose privacy has been impacted by the handling of the personal information of a deceased individual should have standing to lodge a complaint.[127] The Law Council of Australia queried whether it was appropriate to allow third parties to lodge complaints and seek redress for an infringement of another person's privacy.[128]

ALRC's view

8.106 A breach of the provisions relating to the personal information of a deceased individual should be considered an 'interference with privacy' under the *Privacy Act*, giving rise to the right to lodge a complaint with the Privacy Commissioner. The complaint process should parallel, as far as possible, the process provided for complaints by living individuals about the handling of their own personal information by organisations.

8.107 In some circumstances, the relevant 'interference with privacy' will not be an interference with the privacy of the deceased individual. In relation to a denial of access to the personal information of a deceased individual, for example, the ALRC uses the term 'interference with privacy' in a purely technical sense to indicate that an alleged breach of the provision would ground a right to lodge a complaint with the Privacy Commissioner.

8.108 The following individuals should have standing to lodge a complaint about the handling of the personal information of a deceased individual. In relation to an alleged breach of the use and disclosure, access, data quality or data security provisions, the deceased individual's parents, children or siblings who are at least 18 years old, spouse, de facto partner[129] or legal personal representative should have standing to allege an interference with privacy. The relevant proposal in DP 72 did not include the access provision in this list. The ALRC is now of the view that these parties should be able to lodge a complaint with the Privacy Commissioner where, for example, access has been provided to a third party in inappropriate circumstances.

8.109 The ALRC considers that the OVPC's suggestion that this list should be extended to include 'any other individual who, in the opinion of the Privacy Commissioner, has a sufficient interest in the subject-matter of the complaint' has

---

125 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
126 Confidential, *Submission PR 536*, 21 December 2007.
127 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
128 Law Council of Australia, *Submission PR 527*, 21 December 2007.
129 The ALRC recommends that the term 'de facto spouse' in the *Privacy Act* be changed to 'de facto partner': see Rec 63–4.

merit. The ALRC has not, however, had the opportunity to consult on this issue and so is not in a position to make such a recommendation.

8.110 In relation to a request for access to the personal information of a deceased individual, in addition to the parties mentioned above, any person who has made a request for access to the personal information of a deceased individual and has been denied access should have standing to lodge a complaint.

Recommendation 8–3 Breach of the provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner:

(a) in relation to an alleged breach of the use and disclosure, access, data quality or data security provisions—the deceased individual's parent, child or sibling who is aged 18 or over, spouse, de facto partner or legal personal representative; and

(b) in relation to an alleged breach of the access provision—the parties in paragraph (a) and any person who has made a request for access to the personal information of a deceased individual where that request has been denied.

Part B

Developing Technology

9. Overview: Impact of Developing Technology on Privacy

Contents

Introduction

9.1 Developments in technology have always influenced discussions about privacy and the formation of information privacy laws. The first modern academic discussion of privacy in 1890[1] was prompted by concerns about the impact of new technologies on privacy, in particular 'instantaneous photography'.[2] In 1983, concerns about dangers to privacy, including developments in information technology and surveillance technology, led the ALRC to recommend in the Report, *Privacy* (ALRC 22) that legislation containing information privacy principles be introduced.[3] Specific privacy concerns related to developments in technology included: increased storage of personal information; speed at which information could be retrieved; substantial reduction in the cost of handling personal information; enhanced linkages between different

1 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
2 D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 10.
3 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Rec 58.

information systems; aggregation of personal information obtained from different sources; security of information systems; and increased transborder data flows.[4]

9.2 In the Second Reading Speech for the Privacy Bill 1988 (Cth) the then Attorney-General, the Hon Lionel Bowen MP, stated that rapid developments in technology for the processing of information had 'focused attention on the need for the regulation of the collection and use of personal information by government agencies and for an independent community spokesperson for privacy'.[5] In 2000, concerns about the security of personal information disclosed during online transactions provided impetus for the introduction of the private sector provisions of the *Privacy Act 1988* (Cth).[6]

9.3 Two recent reviews have considered privacy and emerging technologies. In 2005, the Office of the Privacy Commissioner (OPC) concluded a review of the private sector provisions of the *Privacy Act* (OPC Review). Also in 2005, the Senate Legal and Constitutional References Committee concluded an inquiry into the *Privacy Act* (Senate Committee privacy inquiry). Both the OPC and the Senate Committee recommended that there should be a wider review of privacy laws in Australia and that this review should consider whether the provisions of the *Privacy Act* remained adequate and effective in light of developments in technology.[7]

9.4 Part B of this Report considers the impact of developing technology on privacy. This chapter provides an overview of several developing technologies. Chapter 10 discusses how best to accommodate developing technology in a regulatory framework. The impact of 'Web 2.0'[8] and how the internet has changed the nature of a 'public' space are discussed in Chapter 11. Finally, Chapter 12 discusses the prevalence of identity theft in the electronic environment.

Privacy-enhancing technologies

9.5 The way that technology is used often determines whether it is privacy enhancing or privacy invasive.[9] Some technologies, known as privacy-enhancing

---

4 Ibid, [5.7]. The ALRC also noted that new small computers 'may provide effective safeguards for privacy because they are not usually interconnected': Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1391]. The ALRC's general approach to technology, however, reflected an awareness of the impact on privacy of future linkages between technical systems. Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Summary of Recommendations.

5 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General), 2118.

6 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15749.

7 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), recs 6, 8; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 1, 69.

8 The term 'Web 2.0' can be used in various contexts. In this Report, it is used to refer to the social phenomenon where internet users—often individuals acting in a personal capacity—upload and distribute content such as text, photographs and videos.

9 See, eg, J Alhadeff, *Consultation PC 169*, Sydney, 26 April 2007; M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002), 9–10.

technologies (PETs), operate to protect privacy. Particular PETs that can be implemented by individuals are discussed throughout this chapter. Chapter 10 discusses the role of PETs in a regulatory framework, as well as the importance of ensuring awareness of PETs and encouraging agencies and organisations to incorporate PETs into technical systems at the stage of design. For example, the United States National Security Agency and members of the information technology industry have developed a system that implements a mandatory access control framework, which provides enforced security settings and prevents the setting of discretionary preferences by a computer application or user.[10] Two other PETs that can be used in the online environment are encryption and identity management, considered in more detail below.

Encryption

9.6 Encryption, a form of cryptography, refers to a sequence of processes that ensure that information stored in electronic form or transmitted over networks such as the internet is not accessible to any person not authorised to view that information. Encryption can be used to convert data into a form which cannot be read without using an appropriate 'key'. A particular form of encryption, public-key cryptography, enables the creation and use of 'digital signatures'—that is, the encryption of data in a message with a private key allocated to a particular sender that assures others that only the sender could have created the message.[11] Encryption, however, does not prevent the deletion of information.

9.7 Encryption systems use either, or both, symmetric or asymmetric key ciphers. Information encoded by a symmetric key cipher requires the decoder of the message to hold a key that is identical to, or readily derived from, the key held by the encoder. An asymmetric key cipher system, such as public-key cryptography, uses a combination of a secret 'private' key and a widely available 'public' key. In this system, information encoded using the public key remains encrypted and secure until a person holding the corresponding private key receives the information and uses the private key to decode the information. In some asymmetric systems, the private key also can be used to encode information so that the corresponding public key can be used to decode the information. This reverse approach provides a 'guarantee of authenticity' rather than an encryption method as any person can decode the information using a public key.[12] In comparison to symmetric key cipher systems, asymmetric systems are complex and slow in execution.[13]

---

10 United States National Security Agency, *Security-Enhanced Linux* (2007) <www.nsa.gov/selinux/> at 24 April 2008.

11 Parliament of Australia—Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society* (2000), [2.77]–[2.113].

12 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 221.

13 United States Department of Commerce—National Institute of Standards and Technology, *Introduction to Public Key [Technology and the Federal PKI Infrastructure]* (2001), 11.

9.8 Symmetric and asymmetric encryption systems can be used in conjunction with mechanisms such as one-way-hash functions to ensure that information stored or transmitted in an encrypted form remains unaltered. A hash function can be applied to data, or a message, to produce data of a fixed bit length—for example, 8, 16 or 32 characters. The hash function condenses the message to a 'hash value' of the original message. In a security system intended to safeguard the integrity of messages against any alteration, a hash value together with an original message is transmitted to a receiver who knows the relevant hash function. The receiver can apply the hash function to the original message to create a second hash value that may be compared against the original hash value. Identical hash values indicate that the original message was not altered in transmission. The message, however, could have been intercepted, altered and a new hash value calculated and added during transmission. To prevent this, the hash value itself may be encrypted before being added to the message for transmission. A receiver who possesses a corresponding cipher key can then decrypt the hash value and compare it against the second hash value that is recalculated from the received message.[14]

Identity management

9.9 The remote nature of online transactions has led many agencies and organisations routinely to require individuals to authenticate their identity during transactions. Arguably, however, it is not always necessary for individuals to identify themselves when engaging in online transactions and it is more desirable for some forms of transactions to be 'pseudonymous'.[15] Pseudonymous transactions could be achieved through the use of 'identity escrow'—that is, a system where a trusted third party holds evidence about a person's identity and issues that person an identifier enabling him or her to conduct transactions with other parties.[16] Identity management systems also could facilitate the use of pseudonyms and partial identities.

9.10 Identity management systems provide a mechanism for establishing trust between individuals, agencies and organisations transacting in the online environment.[17] The Privacy Identity Management for Europe (PRIME) project, for instance, emphasises the privacy-enhancing nature of its identity management project, noting that it allows individuals to minimise the disclosure of their personal

---

14 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 221. In Ch 28, the ALRC recommends that the OPC should develop and publish guidance on the 'Data Security' principle. Among other things, this guidance should address the relevant security measures that can be taken to protect personal information, including privacy enhancing technologies such as encryption: Recommendation 28–3.

15 In Ch 20, the ALRC recommends that the Unified Privacy Principles (UPPs) should contain a principle called 'Anonymity and Pseudonymity' that requires an agency or organisation to give an individual the clear option to interact anonymously or pseudonymously, where this is lawful and practicable in the circumstances: Recommendation 20–1.

16 See, eg, R Clarke, *Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue* (1996) Australian National University <www.anu.edu.au/Roger.Clarke/DV/AnonPsPol.html> at 30 July 2007.

17 Information Integrity Solutions, *Trust and the Critical Role of User Centric ID Management* (2006), 1.

information in the online environment and provides them with technical tools to negotiate privacy preferences with online entities.[18]

9.11 Identity management has been described as a three step process.[19] First, an identity is established, which may require an individual, for example, to choose a password or verify his or her identity in person. Before using an identity, authentication through the presentation of credentials is required. A credential may be something that an individual has, such as a radio frequency identification (RFID) tag; something that an individual knows, such as a password; or something that an individual is, such as a facial biometric or fingerprint.[20] Finally, revocation of identity refers to the removal of an identity when use of that identity is no longer required, such as where a customer changes banks. Revocation of identity is an important measure to reduce identity theft.[21]

9.12 User-centric authentication systems require both an individual and the entity with which the individual is transacting to authenticate their identities. Such mutual authentication projects have emerged as a response to the 'asymmetric sharing of control over personal information … [that] commonly leads to a corresponding asymmetry of risk allocation' in the one-way trust model described above.[22] Microsoft and IBM have both developed user-centric identity management systems.[23]

9.13 A new trend in identity management is the development of the federated identity system.[24] Identity federation systems use a central identity provider to authenticate an individual, who can then access certain other domains without needing to re-authenticate their identity. In an identity federation system, individuals can manage their identities by setting pseudonyms for use in different domains and determining what information can be revealed in different contexts. Standardisation in identity federation systems is required for their effective operation, and this is currently the subject of deliberation in international forums.[25]

---

18 Privacy and Identity Management for Europe (PRIME), *PRIME White Paper v2* (2007), 1.

19 International Telecommunication Union, *digital.life: ITU Internet Report 2006* (2006), 114.

20 Information and Privacy Commissioner of Ontario and A Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (2007) Information and Privacy Commissioner of Ontario, 2.

21 International Telecommunication Union, *digital.life: ITU Internet Report 2006* (2006), 114. Identity theft is discussed in Ch 12.

22 Information Integrity Solutions, *Trust and the Critical Role of User Centric ID Management* (2006), 2.

23 Kim Cameron's '7 Laws of Identity' have been incorporated into Microsoft's 'CardSpace' application: K Cameron, *The Laws of Identity* (2005) Microsoft Corporation; Microsoft Corporation, *Introduction to Windows CardSpace* (2006) <cardspace.netfx3.com/content/introduction.aspx> at 30 July 2007. See too IBM, *Idemix: Pseudonymity for e-Transactions* (2006) <www.zurich.ibm.com/security/idemix/> at 24 April 2008.

24 S Wilson, *Correspondence*, 23 April 2007.

25 International Telecommunication Union, *digital.life: ITU Internet Report 2006* (2006), 115–120.

The internet

9.14 The internet is a worldwide collection of interconnected computer networks based on a set of standard communication protocols. The World Wide Web (the Web)—a global collection of publicly accessible electronic information—is accessed by individual computer 'nodes' that are attached to the internet. An individual computer node could be, for example, a personal computer (PC) or a wireless device such as a mobile telephone. The internet was created in the mid 1980s and widespread use of it commenced in the 1990s. In 2007, a survey conducted by the Australian Bureau of Statistics indicated that 61% of Australians aged over 15 had accessed the internet within the past 12 months.[26]

9.15 The internet can be used for a myriad of social, economic and political transactions. It can be used by individuals to send and receive messages that include text, images and sound (email). It can also be used by individuals and organisations to engage in trade (e-commerce) or to advertise or promote goods or services (e-marketing). Further, it can be used by individuals to communicate with governments and access government services (e-government); to engage in leisure activities, such as online gaming; or to access information for personal purposes. It has been noted that user-generated content (or 'Web 2.0') sites such as MySpace, Facebook, Second Life, LinkedIn and YouTube are increasingly used by individuals for the dissemination of information and for social and professional networking purposes.[27] Increasingly, social, business and political communications take place through user-generated sites, internet chatrooms, webcams and two-way videoconferencing.

Data collection on the internet

9.16 Currently, vast amounts of data are collected about internet users, often without their knowledge or consent. For example, data are often collected about the search terms an internet user has entered into an online search engine; the websites an internet user has visited; and the goods or services an internet user has purchased or inquired about online.[28] Data are also collected about internet users who use tools provided by online search engines, such as free email and map services.[29] These data have the potential to reveal a substantial amount of information about an internet user, including 'information about health, education, credit history, [and] sexual or political orientation'.[30] Information collected about internet users is not usually linked directly to an individual, but rather to a particular computer. This is because each computer connected to the internet is allocated a unique Internet Protocol (IP) address for the

---

26 Australian Bureau of Statistics, *8146.0—Household Use of Information Technology, Australia, 2006–2007* (2007).

27 See, eg, Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007; B Howarth, 'Another Life', *Australian IT* (online), 3 April 2007, <www.australianit.news.com.au>.

28 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 127.

29 See, eg, A Brown, 'Google is Watching …', *The Age* (Melbourne), 2 September 2006, Insight 3.

30 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007),127–128.

duration of each internet session.[31] Some information collected about internet users may be subject to the model Unified Privacy Principles (UPPs).[32]

9.17 Information collected about internet users can be used for a variety of purposes, such as to create a profile of the individual for marketing purposes. In 2007, 65% of respondents to research conducted for the OPC indicated that they had more concerns about their privacy when providing details online rather than in hard copy format.[33] Half of the respondents indicated that they had more concerns about their privacy when using the internet than they did two years previously.[34] This section provides a brief overview of the way in which data about internet users can be collected.

Cookies

9.18 A 'cookie' is a piece of information that is sent from a computer or website to an internet user's browser. The browser stores the information on the internet user's computer. If the user accesses the same website at a later time, the cookie is sent back from the user's computer to the website, thereby indicating that the same user has returned to the same website.

9.19 Cookies are used for a number of purposes, such as to personalise online search engines and store lists of items to be purchased online. Although cookies are principally linked to computers, they can also be linked to an individual in certain circumstances. For example, a cookie could be linked to an individual user if the user provides identifying details, such as his or her name and address, when browsing a website.

9.20 Cookies are often stored on an internet user's computer, and accessed by websites visited by the user, without the user's knowledge or consent. In addition, cookies can, in some circumstances, have a lifespan of several years. It is possible, however, for an internet user to take steps to prevent cookies being stored on his or her computer. For example, if the user's operating system allows it, he or she can limit the lifespan of cookies so that they are only stored for as long as the user's browser is running. Alternatively, an internet user can purchase and install software to assist the user to control the use of cookies when he or she enters the online environment.

---

31 G Greenleaf, 'Privacy Principles—Irrelevant to Cyberspace?' (1996) 3 *Privacy Law & Policy Reporter* 114, 115.

32 In Ch 6, the ALRC recommends an amendment to the definition of 'personal information'. See Rec 6–1.

33 Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007), [12.1].

34 Ibid, [12.1].

Web bugs

9.21 A web bug is a small, invisible image that is included on a web page or email. When a web page containing a web bug is accessed, the web bug collects certain information, such as the IP address of the computer, the time the web page was accessed, and the type of browser used to access it. Web bugs are often used on web pages by third parties, such as advertisers, to track the web pages accessed by users. It has been noted that virus scanners have mixed success in locating web bugs on web pages as it is impractical to scan every web page that is accessed by a user.[35]

9.22 When an email containing a web bug is opened, the sender of the email is informed that the email has been opened and the time at which it was opened. In addition, web bugs can identify the IP address of the computer that opened the email. Web bugs can be used by marketers and 'spammers' to verify the validity of email addresses, or by individuals wishing to be informed of the number of times their email has been forwarded and read.[36]

Hypertext transfer protocol

9.23 Hypertext transfer protocol (HTTP) is a set of rules developed to enable information to be requested and sent on the Web. In order to access a particular web page, an internet user's browser must first request certain information. For example, it must send information about the Uniform Resource Locator (URL) of the web page that the user wishes to access. Further information can also be sent during the request for information, however, such as the email address of the internet user or the last web page viewed by the user.[37] If the last web page viewed by the user was an online search engine, then the search term entered into the search engine is also transmitted.[38] In addition, it is possible for the identity of the user to be disclosed if the user's internet service provider (ISP) does not take steps to prevent this from happening.[39]

Spyware and remote access software

9.24 Software such as remote access software or spyware installed on a computer can enable a third party to view the activity or data on that computer.[40] Remote access software can be used for beneficial purposes, for example, by an employee in an organisation to fix another employee's computer from another location. On the other hand, spyware can be installed without the knowledge or consent of the user of the computer for malicious purposes, such as to collect personal information about the user for the purpose of engaging in fraudulent activities.

---

35 W Caelli, *Correspondence*, 2 April 2007.

36 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 133.

37 Office of the Privacy Commissioner, *Protecting your Privacy on the Internet* <www.privacy.gov.au/internet> at 24 April 2008.

38 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 134.

39 Ibid, 135.

40 Australian Government Department of Communications, Information Technology and the Arts, *Spyware Discussion Paper* (2005), [2.2.2].

9.25 Spyware can be installed on a computer in a number of ways. For example, it can be physically installed by another individual, or installed in the online environment where it may be attached to an email or to downloaded material. In 2005, the Australian Government Department of Communications, Information Technology and the Arts (DCITA) announced the outcome of a review of spyware. DCITA concluded that the most serious and malicious uses of spyware were adequately addressed by existing laws, such as computer offences in the *Criminal Code* (Cth).[41]

Social engineering

9.26 Social engineering practices, such as 'phishing', rely on a person providing information to another person, whether face-to-face, over the telephone or over the internet. Social engineering involves 'human interaction (social skills) to obtain or compromise information about an organization or its computer systems'.[42] Phishing is discussed further in Chapter 12.

Security of the internet

9.27 There is concern about the security of personal information transmitted via the internet, particularly the security of information disclosed during the course of e-commerce. Such information may be intercepted during transmission or accessed in an unauthorised manner when stored electronically. Shortcomings in internet security have prompted research projects such as the 'Clean Slate Program' at Stanford University, which aims to design a new internet that is robust, predictable and 'inherently secure'.[43] This section focuses on internet and computer security. It should also be noted, however, that other technologies—such as wireless networks—have security risks that present significant privacy implications.[44]

9.28 A number of reports suggest that data thieves are increasingly 'hacking' into computer systems.[45] There are a number of ways that 'hackers' can access personal information transmitted over the internet or stored on computer systems. For example, a hacker may infect a computer with spyware that can collect personal information

---

41 Australian Government Department of Communications, Information Technology and the Arts, *Outcome of the Review of the Legislative Framework on Spyware* (2005), [2.3].

42 United States Computer Emergency Readiness Team (US-CERT), *National Cyber Alert System—Avoiding Social Engineering and Phishing Attacks* (2004) <www.us-cert.gov/cas/tips/ST04-014.html> at 24 April 2008.

43 N McKeown and B Girod, *Clean-Slate Design for the Internet—A Research Program at Stanford University: Whitepaper Version 2.0* (2006) Stanford University, 2–3.

44 See, eg, R Naraine, *Wi-Fi Hacking, with a Handheld PDA* (2007) ZDNet <blogs.zdnet.com> at 6 February 2007; D Goodin, 'Flash: Public Wi-Fi Even More Insecure than Previously Thought', *The Register* (online), 2 August 2007, <www.theregister.co.uk>.

45 See, eg, 'The Year Hacking Became a Business', *Australian IT* (online), 30 January 2007, <www.australianit.news.com.au>; J Evers, 'Homeland Security Sees Cyberthreats on the Rise', *CNET News.com* (online), 8 February 2007, <news.com.com>.

displayed on a computer screen or stored on a computer system.[46] More sophisticated hacking techniques include the use of 'rootkits', which can be installed directly in an operating system kernel or system hardware and take over an entire computer system.[47] Rootkits have been described as 'cloaking technologies' since they can operate with other malware to hide 'files, registry keys and other operating system objects from diagnostic, antivirus and security programs'.[48]

9.29 Rootkits can be used to establish 'botnets', which are automated crime networks controlled by 'botherders' who use malware to infect numerous computers. Botnet computers are referred to as 'zombies' because a user of an infected computer generally is unaware that the computer has become part a botnet. Botnets can be used by botherders to carry out distributed denial of service attacks, including phishing and spam attacks and, ultimately, identity theft. The Federal Bureau of Investigation has arrested a number of botherders in the United States. Botherders operate in several nations, however, and effective policing of botnets depends on inter-jurisdictional cooperation.[49]

9.30 Individuals are often advised to use commercially-available programs such as anti-virus and anti-spyware programs to ensure computer and network security.[50] It has been noted, however, that market-based solutions may not provide adequate protection against hackers.[51] Moreover, an online safety study conducted in the United States in 2006 indicates that many individuals incorrectly assume that their anti-virus protection is adequate and up-to-date.[52]

9.31 In Chapter 10, the ALRC recommends that the OPC should develop and publish guidance about technologies that impact on privacy. This guidance should incorporate relevant local and international privacy and security standards.[53] Further, in Chapter 51 the ALRC recommends that the *Privacy Act* be amended to require agencies and organisations to notify the OPC and any affected individuals of data breaches in certain circumstances.[54] This measure is intended to reduce the likelihood of security breaches leading to identity theft.

---

46 W Caelli, *Correspondence*, 2 April 2007.

47 D Fisher, 'Rootkit Dangers at an 'All-time High'', *SearchSecurity.com* (online), 6 February 2007, <searchsecurity.techtarget.com>.

48 Australian Institute of Criminology, *High Tech Crime Brief No 12, 2006—High Tech Crime Tools*, 1 December 2006.

49 See, eg, 'FBI Tackles "Zombie" PC Networks', *Sydney Morning Herald* (online), 17 June 2007, <www.smh.com.au>.

50 See, eg, Australian Government, *Securing Your Computer* (2007) Australian Government Department of Communications, Information Technology and the Arts <www.staysmartonline.gov.au/securing_your_computer> at 24 April 2008.

51 P Croll and W Caelli, *Consultation PC 88*, Brisbane, 13 February 2007.

52 National Cyber Security Alliance and Bank of America, *Online Fraud Report* (2006), 1.

53 Rec 10–3.

54 See Rec 51–1. Identity theft is discussed in Ch 12.

The internet of things or ubiquitous computing

9.32 The United Nations agency for information and communications technologies, the International Telecommunication Union, has predicted that the next development in information transfer will be the 'internet of things'. The internet of things, or ubiquitous computing, will allow the transfer of information between inanimate objects, humans, the internet, intranets and peer-to-peer networks—without the need for personal computers.[55] The internet of things will use wireless technologies such as RFID, which is discussed below, together with smart and sensor technologies and miniaturising technologies such as nanotechnology.[56]

9.33 The internet of things will be based on next generation networks (NGNs), which use 'packet-based' Internet Protocol (IP) technology. Many telecommunications devices currently use the Public Switched Telephone Network (PSTN), which is a 'circuit-switched' network. In NGN networks, linked devices are more mobile than in PSTN networks, and service delivery is not linked to the underlying transport technologies.[57]

9.34 The internet of things could impact on privacy by allowing more information to be collected from an individual without his or her knowledge or consent. In addition, the convergence of technologies in the internet of things means that individuals could be more easily tracked, monitored and profiled.[58] It also has been noted that remote access to sensor networks could impact on security of information, as data thieves could 'collect information from further away and from multiple locations simultaneously'.[59] The European Commission is monitoring these developments and at the end of 2008 intends to issue to the European Parliament a communication on privacy, trust and governance issues related to the internet of things.[60]

Radio frequency identification

9.35 A radio frequency identification (RFID) system consists of a 'transponder', a 'reader' and a 'back office' system. A transponder is a small object—often referred to

---

55 International Telecommunication Union, *The Internet of Things* (2005), 3.

56 For an overview of nanotechnology, see S Wood, R Jones and A Geldart, *Nanotechnology: From the Science to the Social—A Report for the Economic and Social Research Council* (2007) Economic and Social Research Council.

57 International Telecommunication Union, *The Internet of Things* (2005), 4.

58 Ibid, 82–3.

59 Ibid, 83.

60 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework* (2007), 11.

as an 'RFID tag'—that transmits data by emitting radio waves.[61] These data are collected by a device known as a reader. Readers can be mobile, resembling hand-held barcode scanners, or fixed at certain locations, such as the entrance to a warehouse or a vehicle toll gateway.[62] Once data are collected by a reader they are sent to a 'back office'—namely, a data processing system.[63] In June 2006, British Petroleum (BP) commenced a 'mesh network' trial in which RFID tags or 'nodes' communicated information directly to other RFID tags. In this trial, an RFID node transmitted 'details of its environment and content … to all other nodes within a 3-meter range'.[64]

9.36 There are two main types of RFID tags—passive tags and active tags.[65] Passive tags lack an internal power source and can operate only if they are in range of a reader that activates the tag.[66] Accordingly, they have a limited 'read range'. They are relatively inexpensive, however, and have a longer life-cycle than active tags.[67] Active tags have an internal power source (usually a battery) that allows them to emit radio waves.[68] These radio waves can be read if the tag is in range of a reader. The 'read range' of active tags is much greater than that of passive tags (up to several kilometres).[69] Active tags also have larger amounts of memory and better processing capabilities than passive tags.[70]

9.37 RFID tags can be attached to objects, such as clothes, shopping trolleys or plastic cards. They also can be attached to animals and people. Passive tags usually are physically smaller than active tags and can be difficult for an individual to detect. An RFID tag can transmit data that identifies the object or entity to which it is attached, such as a unique serial number. It can also transmit data about the price, expiry date, colour, or date of purchase of a product.[71] If an RFID tag is combined with a sensor, it also can transmit data about its surroundings, such as the temperature in its location or the composition of the atmosphere surrounding it.[72]

---

61 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

62 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [1.1.2].

63 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

64 J Collins, 'BP Tests RFID Sensor Network at UK Plant', *RFID Journal* (online), 21 June 2006, <www.rfidjournal.com>.

65 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [1.1.1].

66 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

67 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [2.1].

68 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

69 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [2.1].

70 Ibid, [2.1].

71 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

72 Australian Government Department of Communications, Information Technology and the Arts, *Getting the Most out of RFID: A Starting Guide to Radio Frequency Identification for SMEs* (2006), 6.

9.38 RFID technology has been in existence since the 1940s.[73] Currently, it has a number of established uses, including facilitating automated payments at vehicle toll booths, enabling people to lock and unlock cars remotely, and enabling people to access secure buildings.[74] Additional uses for RFID technology are being deployed as the cost of the technology decreases.[75] In October 2004, for example, the United States Food and Drug Administration approved the use of a subdermal RFID tag for medical purposes, such as to enable health service providers to obtain identity and health information relating to unconscious patients.[76] It has been predicted that between 2006 and 2016 the value of the RFID market will rise from US$2.77 billion to US$26.23 billion.[77]

9.39 The use of RFID technology can benefit individuals, businesses and governments. RFID technology can benefit individuals in the areas of safety, convenience and accessibility. For example, RFID can be used to trace food, lead to shorter supermarket queues and track patients suffering from Alzheimer's disease.[78] It can also be used by businesses to track products from the point of manufacture to the point of sale, thereby reducing inventory and labour costs, and stock losses.[79] Other applications of RFID technology include:

> prevention of counterfeiting of consumer goods; pinpointing the location of theft; library book check-out; tracking passenger bags in airports; residential garbage collection; sensitive document tracking; asset management; equipment and personnel tracking in hospitals; parcel and post management; livestock management; inmate and guard tracking systems for prison security management; parking permits; tire pressure monitoring; and pharmaceutical labelling for monitoring of location, expiration and anti-counterfeiting.[80]

---

73 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

74 Ibid, 7; Australian Government Department of Communications, Information Technology and the Arts, *Getting the Most out of RFID: A Starting Guide to Radio Frequency Identification for SMEs* (2006), 4.

75 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

76 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.133]–[3.143].

77 IDTechEx, *RFID Market $2.77Bn in 2006 to $12.35Bn in 2010* <www.idtechex.com> at 24 April 2008.

78 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework* (2007), 3–4.

79 Australian Government Department of Communications, Information Technology and the Arts, *Getting the Most out of RFID: A Starting Guide to Radio Frequency Identification for SMEs* (2006), 13–16.

80 G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 307–308.

9.40 It also has been suggested that RFID technology could be used to create 'smart products', such as washing machines that wash garments in accordance with instructions on their RFID tags.[81]

9.41 Some uses of RFID technology raise privacy concerns. In particular, concerns arise about the ability of agencies, organisations or individuals to

> surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; [and] read the details of clothes and accessories worn and medicines carried by customers.[82]

9.42 These concerns are exacerbated by the fact that individuals may not be given notice that the products they purchase or the objects they use contain RFID tags and may not be given the choice to remove or disable RFID tags. Further, individuals may not be able to ascertain when, or how many times, data on an RFID tag have been collected.[83] Technologies have been developed that aim to prevent the unwanted scanning of RFID tags, such as 'blocker tags' which 'impair readers by simulating the signals of many different RFID tags'.[84] An individual may not be aware, however, that a product contains an RFID tag and it may not be practical to purchase and carry an RFID blocker. It has been argued, therefore, that PETs are unable completely to 'assuage the danger to privacy engendered by RFID technology'.[85]

9.43 In 2002, one commentator proposed that organisations wishing to use RFID technology should comply voluntarily with an 'RFID Bill of Rights' that granted consumers the right to:

- know whether a product contains an RFID tag;
- have an RFID tag removed or deactivated at the point of purchase;
- use RFID-enabled services without RFID tags;
- access an RFID tag's stored data; and

---

81 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 8.

82 European Union Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP105 (2005), [1].

83 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 5.

84 Information and Privacy Commissioner Ontario, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (2004), 19. See also, Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 26; G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 315–320.

85 G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 320.

- know when, where and why RFID tags are being read.[86]

9.44 To these, other commentators have added that consumers should have the right to:

- own and use readers that enable them to detect and disable permanently RFID tags;
- know who to contact in order to access information pertaining to them that has been collected by RFID technology; and
- be confident that data is securely transmitted and stored.[87]

9.45 In March 2007, the European Commission issued a Communication on RFID to the European Parliament, noting the need for legal certainty for both investors in, and users of, RFID technology.[88] Further, the European Commission has established a widely constituted RFID Stakeholder Group to discuss security and privacy issues and is conducting public consultations on a draft recommendation that sets out the principles that European public authorities and stakeholders should apply in respect of RFID usage.[89]

Other wireless technologies

9.46 Wireless technologies enable devices to transmit and receive data 'by means of a signal that uses some part of the electromagnetic spectrum'.[90] RFID technology, discussed above, is a wireless technology. 'WiFi' and 'Bluetooth' are examples of other wireless technologies.[91] WiFi technology enables devices to connect to the internet in certain 'hotspots', while Bluetooth technology enables devices to connect to each other across short distances.

---

86 S Garfinkel, 'An RFID Bill of Rights 1' (2002) 105(8) *Technology Review* 35, 35.

87 See Privacy Rights Clearinghouse, *RFID and the Public Policy Void: Testimony of Beth Givens, PRC Director to the California Legislature Joint Committee on Preparing California for the 21st Century* (2003) <www.privacyrights.org/ar/RFIDHearing.htm> at 24 April 2008.

88 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework* (2007), 4–11.

89 European Commission—Information Society, *Policies—Towards an RFID Policy for Europe* (2008) <ec.europa.eu/information_society/policy/rfid/index_en.htm> at 3 April 2008.

90 R Clarke, *Wireless Transmission and Mobile Technologies* (2003) Australian National University <www.anu.edu.au/people/Roger.Clarke/EC/WMT.html> at 24 April 2008.

91 The term 'WiFi' is commonly used to describe wireless local area networks based on a particular standard developed by the Institute of Electrical and Electronics Engineers (the IEEE 802.11 standard), while the term 'Bluetooth' is commonly used to describe wireless personal area networks based on the IEEE 802.15.1 standard. Standards are discussed in Chs 10 and 28.

9.47 Wireless technologies can be used to purchase goods, services or digital content (m-commerce), to enhance business performance (m-enterprise) and to provide services that do not involve commercial transactions, such as mobile banking services (m-services). Wireless devices such as personal digital assistants (PDAs) and mobile telephones are increasingly using similar hardware and software systems to those used in PCs. The use of wireless technologies raises privacy concerns because 'device limitations, along with different network configurations mean that wireless technologies present a higher risk from eavesdropping and hackers'.[92] Further, devices that use wireless technologies are vulnerable to theft and subsequent misuse.

Data-matching and data-mining

9.48 Rapid advances in information and communication technology since the 1970s have enabled agencies and organisations to collect and store vast amounts of personal information. This information is often generated by individuals conducting everyday activities, such as

> withdrawing cash from ATMs; paying with debit or credit cards; using loyalty cards; borrowing money; writing cheques; renting a car or a video; making a telephone call or an insurance claim; and, increasingly, sending or receiving e-mail and surfing the Net.[93]

9.49 In addition, some technologies enable large amounts of personal information to be organised and analysed. Two methods of processing and analysing information are discussed in this section—data-matching and data-mining. This chapter discusses data-matching and data-mining outside the health and research context. A number of models that enable the linking of non-identifiable personal information for the purposes of health and medical research are discussed in Chapter 66.

9.50 Data-matching is 'the large scale comparison of records or files … collected or held for different purposes, with a view to identifying matters of interest'.[94] Developments in information technology in the 1970s made data-matching economically feasible and it is conducted regularly in Australia, particularly by government agencies.[95] Data-matching can be conducted for a number of purposes, including to detect errors and illegal behaviour, locate individuals, ascertain whether a particular individual is eligible to receive a benefit, and facilitate debt collection.[96]

---

92 C Gould and others, 'Mapping the Mobile Landscape in Australia ' (2006) 11 *First Monday* <firstmonday.org/issues/issue11_11/gould/index.html>.

93 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 1.

94 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [14].

95 A Caine, *E-government: Legal and Administrative Obstacles to Sharing Data Held by Australian Government Agencies* (2004) Australian Government Information Management Office.

96 R Clarke, 'Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism' (1995) 4 *Information Infrastructure and Policy* 29, 33.

9.51 Data-mining has been defined as 'a set of automated techniques used to extract buried or previously unknown pieces of information from large databases'.[97] Data-mining can be used in different contexts to achieve different goals. For example, it is increasingly used by organisations to enable them to 'design effective sales campaigns, precision targeted marketing plans, and develop products to increase sales and profitability'.[98] Data-mining can also be used by law enforcement agencies to investigate criminal activities. For example, in 2006 it was reported that the National Security Agency in the United States was collecting telephone records of millions of Americans to analyse calling patterns in an effort to detect terrorist activities.[99]

9.52 There are three main steps in the data-mining process: (1) the data are prepared (or 'scrubbed') for use in the data-mining process; (2) a data-mining algorithm is used to process the data; and (3) the results of the data-mining process are evaluated.[100]

9.53 Data-matching and data-mining practices that involve personal information raise a number of privacy concerns. A major concern is that the practices can reveal large amounts of previously unknown personal information about individuals.[101] This concern is exacerbated by the fact that data-matching or data-mining can occur without the knowledge or consent of the data subject, thereby limiting the ability of the data subject to seek access to information derived from a data-matching or data-mining program.[102]

9.54 Another concern relates to the accuracy of the data derived from a data-matching or data-mining process. Data-matching and data-mining involve using information collected for different purposes and in different contexts.[103] If information is incorrect or incomplete at the time of collection, or ceases to be accurate some time after collection, the information generated by the data-matching or data-mining process will be inaccurate. In the case of data-mining, an additional concern is that it is often difficult to inform the data subject of the exact purpose for which his or her personal information is to be collected or used. This is because data-mining activities aim to discover previously unknown information. Further, there is concern about the storage

---

97 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 4.

98 Ibid, 1.

99 L Cauley, 'NSA has Massive Database of Americans' Phone Calls', *USA Today*, 10 May 2006, <www.usatoday.com>.

100 J Bigus, *Data Mining with Neural Networks* (1996), 10–11, cited in Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 5.

101 V Estivill-Castro, L Brankovic and D Dowe, 'Privacy in Data Mining' (1999) 6 *Privacy Law & Policy Reporter* 33, 34.

102 See, eg, Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 14.

103 See, eg, Ibid, 10–11.

of large amounts of personal information gathered for the purpose of data-matching or data-mining.[104]

Smart cards

9.55 A smart card is usually a plastic card with an embedded microchip that can be programmed to perform multiple and varied functions.[105] A microchip embedded in a smart card can vary in sophistication.[106] Some microchips have memory functions only, while others have 'a micro-controller, various types of memory and an operating system'.[107] It has been noted that 'multi-application smartcards today have approximately the same capabilities and logical powers as the first commercial micro-computers in the mid 1970s'.[108]

9.56 Smart card technology has existed for several decades and has been described as 'technology looking for an application'.[109] Currently, smart card technology has a number of established uses. For example, a Subscriber Identity Module (SIM) card in a mobile telephone uses smart card technology.[110] Smart cards also have a number of nascent uses, including for identity authentication and financial transactions. For example, a smart card could store a cardholder's biometric information in order to enable the cardholder to access a building or computer network. It could also contain an 'electronic purse' that could be used as a substitute for cash in small value transactions, such as for travel on public transport or small retail purchases.[111]

9.57 Smart cards can be divided into two main categories: 'contact smart cards' and 'contactless smart cards'. Information contained on a contact smart card can only be read if the card is inserted directly into a card reader. Contactless smart cards, however, use low-frequency radio waves to communicate with readers. Accordingly, they can be read from a distance.[112]

9.58 The use of smart card technology raises several privacy concerns. One concern is that a particular smart card may be linked to a particular individual, for example, where the individual uses his or her bank account to add value to the card's electronic purse. Widespread use of smart cards that are linked to identifiable individuals may

---

104 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 240.

105 See, eg, S Newman and G Sutter, 'Electronic Payments—The Smart Card: Smart Cards, E-payments, & Law—Part I' (2002) 18 *Computer Law & Security Report* 235, 235; Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), i.

106 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006), [b.6].

107 Ibid, [b.6].

108 Ibid, [b.6].

109 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), 3.

110 S Newman and G Sutter, 'Electronic Payments—The Smart Card: Smart Cards, E-payments, & Law—Part I' (2002) 18 *Computer Law & Security Report* 235, 235.

111 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), i.

112 Council of Europe, *Report on the Protection of Personal Data with Regard to the Use of Smart Cards* (2001).

mean that individuals no longer have the option of transacting anonymously.[113] Further, widespread use of these cards could enable vast amounts of information about the activities of cardholders to be collected and stored. In the future, smart cards could

> generate records of the date, time and location of all movements on public and private transport systems, along with details of all goods purchased, telephone use, car parking, attendance at the cinema, and any other activities paid for by smart cards.[114]

9.59 These records could then be used by smart card operators or third parties for a number of purposes, for example, to generate detailed profiles of individuals to market goods and services to them. They may also be sought by third parties, such as law enforcement agencies.[115]

9.60 Another concern is that smart card schemes that are used by numerous agencies or organisations may lack a central data controller. Accordingly, it may be unclear who is accountable for the use, disclosure, accuracy and security of personal information collected by the smart card system.[116] Concern also has been expressed about the potential for function creep[117] and the ability to read contactless smart cards without the cardholder's knowledge or consent. Finally, the security of a smart card system depends on the reliability and security of the various components of the system—that is, the security of the data pathways between the smart card and any reading, processing, storage or transmission system.

9.61 In 2004, the Council of Europe published a set of guiding principles for the protection of personal information in systems using smart card technology.[118] After acknowledging that the protection of personal information in any smart card system depended 'on many different factors and circumstances', the Council set out 11 principles to be taken into account by those who issue smart cards, as well as other participants in smart card systems, such as project designers and managers.

9.62 Among other things, the principles require the collection of personal information for storage on a smart card to be for 'legitimate, specific and explicit purposes'.[119] They also require a smart card to offer an appropriate level of security given the state of technology, the data stored on the card, the applications of the card, and the security

---

113 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), ii.
114 Ibid, ii.
115 Ibid, ii–iii.
116 Office of the Victorian Privacy Commissioner, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005, [26].
117 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.40], [3.43]–[3.54].
118 Council of Europe, *Guiding Principles for the Protection of Personal Data with Regard to Smart Cards* (2004).
119 Ibid, Principle 2.

risks.[120] Further, the principles require a data subject to be alerted every time personal information is exchanged between a smart card and a smart card system.[121]

9.63 In 2006, the Australian Government released part of a framework to assist agencies seeking to implement smart card technology.[122] The framework requires agencies implementing smart card technologies to include data protection clauses in agreements with third parties about the supply of smart cards and related services, and to undertake privacy impact assessments (PIAs) during the design of smart card systems. It also requires agencies implementing smart card technologies to produce comprehensive privacy policy statements and to revise these statements 'whenever a third party agency adds additional functionality to an existing smartcard deployment'.[123] In June 2007, the Online and Communications Council endorsed the initial stages of the National Smartcard Framework.[124] Currently, the Australian Government is continuing to develop the National Smartcard Framework to 'underpin evidence of identity and service initiatives by articulating a minimum set of requirements for interoperability at both the infrastructure and application levels'.[125]

Biometric systems

9.64 Biometric systems enable unique behavioural or physiological attributes of people to be used for identification and authentication.[126] Major biometric technologies include finger scanning, facial recognition, iris and retinal scanning, finger geometry, voice recognition and dynamic signature verification.[127] Other biometric technologies include ear geometry, body odour measurement, keystroke dynamics and gait recognition.[128] In addition, palm vein biometric systems are being developed for application in Automated Teller Machine (ATM) transactions.[129]

9.65 In a typical biometric system, a biometric device, such as a finger scanner, is used to take a biometric sample from an individual.[130] Data from the sample are then analysed and converted into a biometric template, which is stored in a database or an

120 Ibid, Principle 6.
121 Ibid, Principle 9.
122 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006).
123 Ibid, [a.17].
124 Online and Communications Council, 'Fourteenth Online and Communications Council Communiqué' (Press Release, 14 July 2007).
125 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2007) <www.agimo.gov.au/infrastructure/smart_cards> at 24 April 2008.
126 Biometrics Institute, *Biometrics Institute Ltd* <www.biometricsinstitute.org> at 5 May 2008; Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 10–11; Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [16].
127 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.
128 Ibid, 4.
129 Fujitsu, *R&D—Fujitsu Palm Vein Technology* (2007) <www.fujitsu.com/global/about/rd/200506palm-vein.html> at 24 April 2008.
130 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.

object in the individual's possession, such as a smart card.[131] Later biometric samples taken from the individual then can be compared to the stored biometric information to determine who the individual is (identification, or one-to-many matching) or to attempt to authenticate or verify that an individual is who he or she claims to be (verification, or one-to-one matching).[132] One-to-one systems currently provide higher accuracy of matches, although the accuracy of biometric systems varies greatly between systems.[133]

9.66 Biometric technologies have existed for decades.[134] The use of biometric technologies is increasing, however, because of globalisation, developments in information technology, and the desire to identify individuals in order to manage security threats such as terrorism.[135] Biometric systems enable the identity of an individual to be ascertained or authenticated with a fair degree of certainty. Further, advances in biometric technologies mean that biometric systems are now automated, allowing for 'mass identity checks within seconds … with a sufficient degree of certainty'.[136] For this reason, biometric technologies are increasingly used in identification systems, along with other passwords or identity objects, such as smart cards.[137]

9.67 Since 2003, members of the European Union have been required to take fingerprints from all asylum seekers over the age of 14. These fingerprints are then compared to those in a centralised database to determine whether an asylum seeker has previously sought asylum in another Member State.[138] In addition, in 2003, the International Civil Aviation Organisation (ICAO) published 'a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs)'. The ICAO standards require MRTDs to include a facial image in a contactless chip.[139]

9.68 Biometric systems are also being introduced by the Australian Government. For example, in 2003, legislation was passed enabling officials to collect certain types of biometric information from non-citizens in Australia.[140] The legislation aims to ensure that non-citizens are identified accurately in order to enable officials to prevent identity

---

131 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [16]; Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.

132 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.

133 See, eg, Y Wei Yun, *The '123' of Biometric Technology* (2002), 91–93.

134 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [8].

135 Ibid, [12].

136 Ibid, [8].

137 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 13–14.

138 European Commission, *EURODAC: The Fingerprint Database to Assist the Asylum Procedure* (2004).

139 International Civil Aviation Organization, *ICAO Recommendation* <mrtd.icao.int> at 24 April 2008.

140 *Migration Act 1958* (Cth) ss 5A, 40, 46, 166, 170, 172, 175, 188, 192.

fraud in the visa application process, to determine which non-citizens are of national security concern, and to detect forum shopping by visa applicants.[141] Further, in October 2005, the Australian Government introduced the 'ePassport'—a passport with an embedded microchip containing, among other things, a digitised facial image of the passport holder.[142] From 2007, those holding an ePassport could use an automated border security system called 'SmartGate' in two airports in Australia. The SmartGate system uses facial recognition technology to perform the customs and immigration checks normally performed by Australian customs officers.[143] Australian ePassport holders will also be able to participate in the United States Visa Waiver Program.[144]

9.69 Biometric systems increasingly are being used or contemplated by organisations, including in methadone programs, taxi booking services, ATMs and online banking, and access to buildings.[145]

9.70 The use of biometric technologies raises a number of privacy concerns. These may vary according to the context in which the biometric information is collected and the type of biometric system in operation.[146] Some of the general concerns are as follows.

9.71 First, there is a concern that widespread use of biometric systems will enable extensive monitoring of the activities of individuals.[147] This is so particularly if the same form of biometric information is used to identify individuals in a number of different contexts—that is, if a type of biometric information is used as a unique multi-purpose identifier.[148] Secondly, there is a concern that biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent.[149] Thirdly, there is a concern that biometric information could reveal sensitive personal information, such as information about a person's health or religious beliefs.[150] Fourthly, there is a concern that the security of biometric systems

---

141 Explanatory Memorandum, Migration Legislation Amendment (Identification and Authentication) Bill 2003 (Cth).

142 A Downer (Minister for Foreign Affairs), 'Australia Launches ePassports' (Press Release, 25 October 2005).

143 Australian Customs Service, *SmartGate* (2006) <www.customs.gov.au/site/page.cfm?u=4243> at 4 September 2006.

144 United States Government Department of State, *Visa Waiver Program (VWP)* (2006) <travel.state.gov/visa/temp/without/without_1990.html> at 24 April 2008.

145 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 240.

146 M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

147 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12.

148 M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002). Multi-purpose identifiers are discussed further in Ch 30.

149 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12–13.

150 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), 6; M Crompton, 'Biometrics and Privacy: The End

could be compromised and that biometric information stored in a central or local database, or on an object in the possession of an individual, could be acquired by those wishing to use it for some kind of gain.[151] Finally, the accuracy and reliability of many biometric systems are still unknown,[152] causing some to express concern about the potentially serious consequences for an individual who is falsely accepted or rejected by a biometric system.[153]

9.72 The Council of Europe has cautioned that biometric systems should not be implemented for the mere sake of convenience.[154] It has recommended that before introducing a biometric system

> the controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider possible alternatives that are less intrusive for private life.[155]

DNA-based technologies

9.73 It has been argued that DNA-based technologies differ from biometric technologies because they require actual physical samples to be taken from a person, as opposed to the taking of an image or scan of a person; and because DNA matching is not automated or done in real time.[156] The use of DNA-based technologies, however, raise a number of the same privacy issues as are raised by the use of biometric technologies.

Genetic samples

9.74 In 2003, the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council released *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96). The report was the product of a joint two-year inquiry into the legal and ethical issues surrounding human genetic information. In this report the ALRC and AHEC considered the privacy of human genetic samples, an issue that is discussed further below, and the privacy of human genetic information, which is discussed in Part H.

---

of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

151 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 13–15.

152 Ibid, 36.

153 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005); Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 10.

154 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [107].

155 Ibid, [107].

156 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.

9.75 The ALRC and AHEC concluded that the *Privacy Act* did not cover genetic samples. This was because it was unlikely that genetic samples constituted 'information', or information stored in a 'record', for the purposes of the *Privacy Act.* Further, an unidentified and uncoded genetic sample might not constitute 'personal information' for the purposes of the Act.[157]

9.76 The ALRC and AHEC, therefore, recommended that the *Privacy Act* be amended to extend the coverage of the Information Privacy Principles (IPPs) and the NPPs to identifiable genetic samples. In particular, the ALRC and AHEC recommended that: the definition of 'personal information' be amended to include bodily samples from an individual whose identity was apparent or could reasonably be ascertained from the sample; and that the definition of a 'record' be amended to include a bodily sample.[158]

9.77 The ALRC and AHEC also recommended that the *Privacy Act* be amended to provide that an individual had a right to access part of his or her own bodily samples, through a nominated medical practitioner, for the purpose of medical testing, diagnosis or treatment. Access could be refused, however, in certain circumstances.[159]

9.78 Finally, the ALRC and AHEC recommended that the *Privacy Act* be amended to enable an individual to access part of a bodily sample of his or her first-degree genetic relatives, through a nominated medical practitioner, where such access was necessary to lessen or prevent a serious threat to his or her life, health, or safety. An organisation subject to the *Privacy Act* that received such a request would be obliged to seek consent from the genetic relative, where practicable, before determining whether to provide access. Again, access could be refused in certain circumstances, including when it would have an unreasonable impact upon the privacy of the individual from whom the sample was taken.[160] The Australian Government rejected these recommendations and, to date, they have not been implemented.[161] The ALRC has not revisited these issues in the current Inquiry.

Voice over Internet Protocol

9.79 Voice over Internet Protocol (VoIP) enables spoken conversations to be conducted in real time over the internet.[162] It is a subset of technology referred to as 'IP Telephony', which enables facsimile messages, video and other forms of data traditionally transmitted via the PSTN to be transmitted via the internet. IP telephony also enables the transmission of television and radio services.

---

157 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [8.4]–[8.26].

158 Ibid, Rec 8–2.

159 Ibid, Rec 8–3.

160 Ibid, Rec 8–4.

161 Australian Government Attorney-General's Department, *Government Response to Australian Law Reform Commission and Australian Health Ethics Committee Report: Essentially Yours: The Protection of Human Genetic Information in Australia* (2005) <www.ag.gov.au> at 24 April 2008.

162 For example, Skype software enables users to access VoIP services.

9.80 VoIP technology transmits the sound waves of speech via the internet in the form of IP data packets.[163] It enables users to avoid the costs of communicating over long distances that are often incurred with traditional telecommunications carriers. It also enables users to encrypt telephone conversations and conduct telephone conversations with groups of people. VoIP technology can offer a variety of services, including 'peer-to-peer services'—that is, services that are isolated from the traditional PSTN. These allow users to make and receive calls only over the internet.[164] Alternatively, VoIP technology can offer 'any-to-any connectivity' services, allowing users to make and receive calls to and from any telephone number.[165]

9.81 VoIP services usually will be classified as carriage services for the purposes of the *Telecommunications Act 1997* (Cth).[166] This means that VoIP service providers generally will be 'carriage service providers' that are required to observe the provisions in Part 13 of the *Telecommunications Act* that protect the confidentiality of telecommunications information. These provisions are discussed in Part J. If, however, a VoIP service does not connect with the PSTN at all, the service provider may not be regulated by the *Telecommunications Act* but may be regulated by the *Privacy Act.*[167]

9.82 A concern that has arisen in relation to VoIP technology is that Australians may access VoIP services from providers outside Australia.[168] This may impact on the standards of protection for personal information disclosed during a VoIP call.[169] The OPC Review recommended that the Australian Government initiate discussions in international forums to deal with international jurisdictional issues arising from the global reach of new technologies such as VoIP.[170] VoIP technology is discussed further in Part J.

Location detection technologies

9.83 A number of technologies can provide real time information about the location of devices, and hence the location of users of the devices. The types of devices that can be located include mobile telephones, laptop computers, personal digital assistants and

163 Australian Government Department of Communications, Information Technology and the Arts, *Examination of Policy and Regulation Relating to Voice Over Internet Protocol (VOIP) Services* (2005), 14.
164 Ibid, 14–15.
165 Ibid, 15.
166 Ibid, 19.
167 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 26.
168 Ibid, 25.
169 Ibid, 25.
170 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 70.

gaming consoles.[171] Location detection technologies, such as the global positioning system (GPS), are included as a standard feature in many new mobile telephones.

9.84 The accuracy of location information varies depending on the location detection technology used. For example, the GPS is a network of 24 satellites established and operated by the United States Department of Defense.[172] Each satellite emits a signal that can be detected by a receiver. The satellites are positioned so that a minimum of four can be detected simultaneously by a receiver anywhere on the Earth's surface.[173] A receiver can determine its location with a high degree of accuracy by calculating the amount of time it takes for the signals emitted by the satellites to reach it.[174] Alternatively, the location of a mobile telephone can be determined with a moderate degree of accuracy by calculating the time a signal takes to receive three or more base stations.[175] Geo-location technologies can determine the location of an individual's IP address with a degree of accuracy that, depending on source and circumvention factors, ranges from country to city to street level.[176]

9.85 Location detection technologies and other wireless technologies allow 'location-based services' to be provided to individuals.[177] There are many types of location-based services, including services that assist individuals to travel to particular locations; inform individuals about local conditions, such as traffic and weather conditions; provide individuals with information about goods or services in their immediate vicinity, and target advertising of goods and services to individuals on the basis of their location.[178]

9.86 Location detection technologies also may enhance service delivery by emergency services. Emergency call persons in Australia utilise subscriber information in the Integrated Public Number Database to determine the location of users of fixed telephone lines.[179] They are unable, however, to determine accurately the location of users of mobile telephones.[180] In the United States, mobile telephone providers are required to provide emergency call persons with precise information about the location of the mobile telephone used to call the emergency service.[181]

---

171 S Benford, *Future Location-Based Experiences* (2005) Joint Information Systems Committee Technology and Standards Watch, 4.

172 Australian Communications Authority, *Location Location Location* (2004), 32.

173 Ibid, 32.

174 Ibid, 33.

175 Ibid, 31, 34.

176 D Svantesson, *Geo-identification—Now They Know Where You Live* (2004) Bond University Faculty of Law, 2.

177 S Benford, *Future Location-Based Experiences* (2005) Joint Information Systems Committee Technology and Standards Watch, 4.

178 See, eg, Ibid, 4; M James, *Where are You Now? Location Detection Systems and Personal Privacy* (2004) Parliamentary Library—Parliament of Australia.

179 Australian Communications Authority, *Location Location Location* (2004), 17. The Integrated Public Number Database is discussed in Part J.

180 Ibid, 18.

181 See Federal Communications Commission, *Enhanced 911—Wireless Services* (2006) <www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html> at 24 April 2008.

9.87 Location detection services enable the location of individuals to be determined in real time. Further, they generate records of the physical movements of individuals. For this reason, they have the potential to impact significantly on privacy. By analysing information about the location of an individual, a third party may derive or infer personal information about an individual, such as information about his or her consumer preferences or social activities.

9.88 The European Union Directive on privacy and electronic communications deals explicitly with 'location data' in the electronic communications sector.[182] Location data is defined as 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.[183] The Directive prohibits the processing of location data that has not been anonymised without the consent of the user of the service.[184] It also requires service providers to inform users, before obtaining their consent, of the type of location data to be processed, the purpose and duration of the proposed processing, and whether the data will be transmitted to a third party for the purpose of providing a value added service.[185] Users must be given the opportunity to withdraw their consent at any time to the processing of location data.[186] Further, processing of the data must be restricted to that which is necessary for the purposes of providing the value added service.[187] Location detection technologies are discussed further in Part J.

Surveillance technologies

9.89 Surveillance involves the monitoring of a person, place or object to obtain certain information or to alter or control the behaviour of the subject of the surveillance.[188] Surveillance can be covert or overt, and can be conducted by a variety of individuals, agencies or organisations for different reasons. For example, surveillance can be conducted by law enforcement agencies to prevent or investigate crime, by media organisations to obtain commercially valuable information, or by individuals to monitor the activities of family members. The practice of surveillance is antithetical to privacy because the goal of surveillance is to 'pierce the privacy shield'.[189] While surveillance is said to be 'at least as old as recorded history',[190]

182 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002).
183 Ibid, art 2.
184 Ibid, art 9(1).
185 Ibid, art 9(1).
186 Ibid, art 9(1), (2).
187 Ibid, art 9(3).
188 R Clarke, *Have We Learnt to Love Big Brother?* (2005) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html> at 30 April 2008.
189 New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001), [1.5].
190 Ibid, [1.18].

developments in surveillance technology and the increased availability of this technology pose significant risks to privacy.

9.90 In ALRC 22, the ALRC considered the use of listening devices. It concluded that, as a general principle, an individual's private communications should not be monitored without his or her consent.[191] Accordingly, it recommended that legislation prohibit the use of listening devices for non-consensual or secret surveillance,[192] with some exceptions for the use of listening devices for law enforcement purposes and for 'participant monitoring'.[193]

9.91 In ALRC 22, the use of optical surveillance devices was also considered. The ALRC noted that the 'growth and increased sophistication of modern technological surveillance devices make it imperative that some legislative control be imposed on their use for optical surveillance'.[194] The ALRC concluded that there should be no regulation of optical surveillance in public places—where individuals could expect to be observed—but recommended that the use of optical surveillance devices to observe people who would otherwise reasonably expect to be safe from observation be prohibited.[195] The ALRC recommended that there should be exceptions to the general prohibition on optical surveillance in private places, such as an exception for the use of an optical surveillance device by a person for the purpose of observing what, on reasonable grounds, appeared to be the commission of an offence, and an exception for the use of an optical surveillance device for law enforcement purposes.[196]

9.92 There are infinite innovations in the design of surveillance technologies. Some surveillance technologies, such as Closed Circuit Television (CCTV), can be combined with software that operates automatically to detect certain matters of interest.[197] For example, CCTV surveillance systems can be used in combination with character recognition technologies to enable automatic number plate recognition. Automatic number plate recognition systems extract the text of number plates from visual images of cars for a number of purposes, such as to compare them to records of stolen vehicles and unregistered cars.[198] Intelligent software can reduce the need for live monitoring of surveillance systems and reduce costs associated with recording irrelevant activity.[199]

---

191 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1122].
192 Ibid, Recs 28, 30.
193 Ibid, Recs 29, 40–50. Participant monitoring can occur: when a party to a private conversation uses a listening device to record the conversation without the consent of the other party; and when a party to a private conversation uses a listening device to transmit the conversation to someone who is not a party. Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1127].
194 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1187].
195 Ibid, Recs 52, 53.
196 Ibid, Recs 53, 54.
197 Council of Australian Governments, *A National Approach to Closed Circuit Television* (2006), 18.
198 See, eg, T Holding (Victorian Minister for Police and Emergency Services), 'Government to Keep Eye on Number Plate Trial' (Press Release, 16 March 2005).
199 Council of Australian Governments, *A National Approach to Closed Circuit Television* (2006), 18.

9.93 The use of surveillance devices by federal law enforcement officers is regulated by the *Surveillance Devices Act 2004* (Cth). A surveillance device is defined as 'a data surveillance device, a listening device, an optical surveillance device or a tracking device', a device that is a combination of any two or more of these types of devices, or a device prescribed by regulations.[200] Generally, federal law enforcement officers must obtain a warrant to use a surveillance device. In certain circumstances, however, a surveillance device can be used without a warrant if use of the device does not involve entry onto premises, or interference with any vehicle or thing, without permission.[201] In addition, a listening device can be used without a warrant if an officer is participating in the conversation.[202] The use of surveillance devices by the Australian Security Intelligence Organisation is regulated by the *Australian Security Intelligence Organisation Act 1979* (Cth), while the intelligence gathering functions of the Australian Secret Intelligence Service and the Defence Signals Directorate are set out in the *Intelligence Services Act 2001* (Cth).

9.94 The handling of personal information obtained by the use of surveillance devices is generally regulated by the *Privacy Act* when the use of the device involves the collection of personal information for inclusion in a record. As noted in Chapter 1, the Victorian Law Reform Commission is currently examining surveillance in public places as part of a larger inquiry into privacy. It is anticipated that the recommendations resulting from this inquiry will be considered by the Standing Committee of Attorneys-General. In Chapter 73, the ALRC discusses access to and interception of information under the *Telecommunications (Interception and Access) Act 1979* (Cth).

Other developing technologies

9.95 There are other developing technologies that have the potential to impact adversely on privacy. For example, it has been argued that electronic number mapping (ENUM) may provide agencies, organisations and individuals with increased ability to track others.[203] ENUM is 'an electronic numbering system that can link the public telephone network and the internet by allowing telephone numbers to be converted into internet domain names'.[204] In summary, ENUM enables telephones connected to the internet to make calls to the PSTN and receive calls from the PSTN.[205]

---

200 *Surveillance Devices Act 2004* (Cth) s 6(1).
201 Ibid ss 37–39.
202 Ibid s 38.
203 R Clarke, 'ENUM—A Case Study in Social Irresponsibility' (2003) 9 *Privacy Law & Policy Reporter* 181, 181.
204 Australian Communications Authority, *Annual Report 2004–05* (2005), 36.
205 Australian Communications and Media Authority, *What is ENUM or Electronic Number Mapping?* <www.acma.gov.au> at 30 July 2007.

9.96 The Australian Communications and Media Authority (ACMA) submitted that the next development in ENUM technology, infrastructure ENUM, will involve the mapping of blocks of ENUM registrations 'to a single Internet resource—generally a Voice over Internet Protocol (VoIP) address'.[206] One application of infrastructure ENUM could involve the 'peering'—or direct connection—of VoIP services in isolation from the PSTN.[207] In Chapter 71, the ALRC notes that ACMA recently commissioned a PIA for its ENUM project.[208] The PIA contained 13 recommendations relating to the implementation of the project. The ALRC understands that ACMA is in the process of implementing these recommendations.[209]

9.97 Digital Rights Management (DRM) technologies also have the potential to impact adversely on privacy. DRM technologies enable copyright owners to protect digital material by controlling the ways in which the material is accessed, used, copied and distributed.[210] It has been noted that virtually all DRM technologies require the collection of personal information about consumers of copyright material.[211] Accordingly, they limit the ability of these consumers to access material anonymously.

9.98 Further, DRM technologies can be used to monitor the activities of consumers by collecting information about the 'content used, the time of use, the frequency of use, and the location of use'.[212] The Australia–United States Free Trade Agreement requires the parties to introduce a scheme imposing liability for activities relating to the circumvention of 'effective technological measures' used by copyright owners to

---

206 Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007.

207 See, eg, Australian Communications and Media Authority, *Australian ENUM News* (2006) <www.acma.gov.au/WEB/STANDARD//pc=PC_2328> at 30 April 2008.

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

209 Australian ENUM Discussion Group, *Evaluation of the Australian ENUM Trial* (2007), Appendix B.

210 Information and Privacy Commissioner Ontario, *Privacy and Digital Rights Management (DRM): An Oxymoron?* (2002), 2.

211 Ibid, 4.

212 D Mulligan, J Han and A Burstein, 'How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use"' (Paper presented at Proceedings of the 3rd ACM Workshop on Digital Rights Management, Washington DC, 27 October 2003).

protect their material.[213] In December 2006, the *Copyright Amendment Act 2006* (Cth) amended the *Copyright Act 1968* (Cth) and the *Copyright Regulations 1969* (Cth) to implement this requirement of the Australia–United States Free Trade Agreement.[214]

9.99 Another area of concern relates to the use of application service providers. An application service provider is a business that enables customers to access software applications over a network, typically the internet. Use of an application service provider may result in large amounts of a customer's data being stored remotely.[215] In Chapter 10, the ALRC considers how best to accommodate these technologies in a regulatory framework.

213 *Australia-US Free Trade Agreement*, 18 May 2004, [2005] ATS 1, (entered into force generally on 1 January 2005), art 17.4.7.

214 *Copyright Amendment Act 2006* (Cth).

215 See, too, the discussion of cross-border data flows in Ch 31.

10. Accommodating Developing Technology in a Regulatory Framework

Contents

Introduction

10.1 This chapter sets out how the ALRC has addressed the impact of developing technology on privacy. The recommendations that are made in this chapter are situated within the ALRC's general approach to privacy regulation, which is discussed in detail in Chapters 4 and 18 of this Report. In summary, the ALRC recommends a hybrid regulatory model that draws heavily on principles-based and compliance-oriented regimes. The ALRC's view is that a pure principles-based model will not always meet

the policy objectives of privacy regulation. The ALRC recommends a combination of the following:

- primary legislation;
- regulations and other legislative instruments; and
- guidance issued by the Office of the Privacy Commissioner (OPC).

10.2 The key finding in this chapter is that the model Unified Privacy Principles (UPPs) should be technology neutral. Several mechanisms that will ensure that the privacy regulatory framework remains technology *aware* are recommended. Several recommendations that relate to the role of the OPC in protecting individual privacy in light of technological developments are made. The importance of proactive mechanisms such as Privacy Impact Assessments (PIAs), research and monitoring, international engagement, guidance and education is also emphasised. Underpinning the recommendations in this chapter is a focus on privacy-enhancing technologies (PETs) and the deployment of technology in a privacy-enhancing way. Finally, the chapter summarises relevant amendments to the primary legislation that are recommended in other chapters of this Report.

Should the *Privacy Act* be technology neutral?

10.3 The explanatory memorandum to the Privacy Amendment (Private Sector) Bill 2000 noted that the National Privacy Principles (NPPs) were intended to be technology neutral. Technology-neutral privacy principles were intended to ensure that the *Privacy Act* remained flexible and relevant in the case of technological change.[1] In Chapter 9, the ALRC considers the impact on privacy of several new and developing technologies. These technologies facilitate easier, cheaper and faster methods by which information may be collected, accessed, aggregated and communicated. Further, there is an increasing ability to store large quantities of information. In its submission, the OPC cited a University of California, Berkeley, study that found that only 0.01% of all new information produced in 2002 was paper-based.[2] The OPC submitted that the privacy regulatory framework should be informed by the assumption that 'information will be handled in electronic form'.[3]

10.4 In light of these technological developments, the ALRC asked in the Issues Paper, *Review of Privacy* (IP 31) whether the *Privacy Act* should remain technology neutral.[4] In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC noted some opposition to the proposition. For example, Professor Roger Clarke

1 Further Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 9.
2 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
3 Ibid.
4 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 11–4.

queried whether the concept of technology neutrality operates effectively in practice.[5] Clarke has noted previously that the impact of some technologies on privacy may be inconceivable until the technologies have actually been invented and deployed.[6]

10.5 The ALRC, however, proposed in DP 72 that the *Privacy Act* should remain technology neutral.[7] In making this proposal, the ALRC expressed the view that current technologies do not alter fundamentally the nature of the information-handling cycle. For example, technology such as surveillance devices and radio frequency identification (RFID) systems may facilitate the collection of personal information without the knowledge or consent of an individual, but the collection of the information will still be regulated by the 'Collection' principle in the model UPPs. The ALRC expressed the view that the handling of personal information by developing technologies can be regulated by high level and technology-neutral UPPs, although it may be necessary to make some amendments to the *Privacy Act* to ensure that the Act remains technology aware.

Submissions and consultations

10.6 There was strong support for this proposal.[8] Medicare supported a technology-neutral *Privacy Act* as 'it would be impossible for legislation to keep up with the rapid pace at which technology keeps evolving'.[9] Optus submitted that '[t]he current

---

5 R Clarke, *Consultation PC 14*, Canberra, 30 March 2006.

6 R Clarke, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 25 February 2005, 2.

7 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–1. This proposal was consistent with the views of the majority of stakeholders that responded to IP 31. See, eg, Australian Communications and Media Authority, *Submission PR 268*, 26 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Telstra, *Submission PR 185*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Australian Retailers Association, *Submission PR 131*, 18 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007; M Fenotti, *Submission PR 86*, 15 January 2007; Australia Post, *Submission PR 78*, 10 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

8 See Australian Government Department of Human Services, *Submission PR 541*, 21 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; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; ANZ, *Submission PR 467*, 13 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; Communications Alliance Ltd, *Submission PR 439*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Australian Bureau of Statistics, *Submission PR 383*, 6 December 2007; AAPT Ltd, *Submission PR 338*, 7 November 2007.

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

principles based, technology neutral regime provides a powerful framework on which to base privacy requirements when assessing new and emerging technology'.[10]

10.7 A number of stakeholders supported the proposal but noted that the effectiveness of a technology-neutral *Privacy Act* will be dependent upon the technology-aware framework underpinning the legislation. For example, the Department of Finance and Deregulation supported the proposal 'in principle', but noted that legislation that does not

> apply to any specific technology can still significantly affect how technology operates or is employed. It may be arguable as to whether such legislation is really technologically neutral if it deliberately or unintentionally limits or affects the use or operation of technology.[11]

10.8 The Public Interest Advocacy Centre (PIAC) highlighted the important role of the regulator in a technology-aware privacy regime. PIAC submitted that the OPC should play a more proactive role in the exercise of its research and monitoring function with regard to the impact on privacy of new and emerging technologies.[12] The Australian Privacy Foundation submitted that the ALRC's final recommendation should acknowledge that the overall privacy regulatory framework 'should be designed so as to ensure ongoing awareness of the impacts of technology, and to avoid blindness to them'.[13]

ALRC's view

10.9 In the ALRC's view, technology-neutral privacy principles provide the most effective way to ensure individual privacy protection in light of developing technology.[14] It would be undesirable to recommend significant changes to the UPPs to accommodate technologies, which are yet to be invented or deployed. Further, where possible, provisions of the *Privacy Act* should be technology neutral.[15] This approach does not foreclose the possibility of technology-specific regulation or legislative instruments in certain circumstances. The Biometrics Institute Privacy Code is an example of a Part IIIAA code that was initiated by the biometrics industry and, following approval by the OPC, became a legislative instrument.[16] If the OPC found it necessary to initiate a code to address the handling of personal information using a

---

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

11 Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008.

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

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

14 This recommendation is made in Ch 18: Rec 18–1. In a submission to IP 31, Professor William Caelli queried whether any legislation could truly be 'technology neutral', submitting that 'artefact neutral', meaning no reference to any specific manifestation of technology, would be the more correct term: W Caelli, *Submission PR 99*, 15 January 2007. The ALRC accepted Professor Caelli's point but decided to use the term 'technologically neutral' as it is the more commonly understood term. The ALRC notes, however, that technologically neutral UPPs do not preclude the use of words such as 'technology'.

15 See, eg, Rec 47–1.

16 The ALRC discusses Part IIIAA codes in Ch 48.

certain technology, such as RFID, the OPC could lobby the minister responsible for administering the *Privacy Act* to have such a code included in regulations.[17]

10.10 Technology-specific regulations or other legislative instruments of this nature are consistent with the ALRC's three-tiered approach to privacy regulation, and do not represent a failure of technology-neutral UPPs. Instead, such regulations indicate that information handled by particular technologies may require stronger protection in certain, limited circumstances. Further, to ensure the effectiveness of technology-neutral privacy principles, the OPC should provide technology-specific guidance on meeting the requirements in the model UPPs when certain technologies are used to handle personal information.

10.11 One of the OPC's functions is to research and monitor developments in technology and to report to the minister responsible for administering the *Privacy Act*.[18] In the ALRC's view, the OPC could exercise this function to provide a continuing review mechanism of the adequacy and effectiveness of the *Privacy Act* in light of further developments in technology.

10.12 A number of concerns raised by stakeholders in this Inquiry about the impact of technology on privacy are dealt with in other sections of this Report. In Part A, the ALRC recommends amendments to the definitions of 'personal information', 'sensitive information' and 'record'. In Part D, the ALRC makes a number of recommendations concerning the content of the model UPPs. In Part F, the ALRC recommends additional OPC powers and functions that are relevant to technological developments. These recommendations are discussed below, and in Chapter 11.

Key themes in a 'technology aware' framework

10.13 Professor Lawrence Lessig has described four modes of regulation in cyberspace, noting that these modes are reflected in 'real space':

- **law—**which may include prohibitions and sanctions for online defamation and copyright infringement;

- **social norms—**which may involve a user ensuring that the behaviour of their avatar conforms to community expectations in an online world such as Second Life or a social networking site such as Facebook;

---

17 In Ch 5, the ALRC 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 on agencies and organisations: Rec 5–1.

18 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

- **markets—**which regulate the price paid for access to the internet and access to information on the internet; and

- **architecture—**which is the code, hardware or software that shapes the appearance of cyberspace.[19]

10.14 Cyberspace regulatory theorists disagree on the role that should be taken by each modality in Lessig's analysis.[20] Lessig demonstrates, however, that regulation of the internet and other developing technologies must be through measures additional to conventional law. Otherwise, the regulation through law can be circumvented or undermined, for example, by the architecture of the internet.

10.15 As a starting point, the ALRC suggests that broadly drafted statutory principles could address the impact of developing technology. A regulatory framework, however, should also accommodate co-regulation between the OPC and agencies and organisations, and it should seek to empower individuals by providing them with the requisite knowledge of how to protect their privacy.

10.16 A technology-aware regulator plays a crucial role in dealing with the impact of technology on privacy. In this chapter, the ALRC recommends that the OPC should provide guidance that outlines how certain requirements in the model UPPs can be met by agencies and organisations that use particular technologies to handle personal information.[21]

10.17 Education is a further important feature of the regulator's role. In this chapter, the ALRC recommends that the OPC should educate individuals about how PETs can be used to protect privacy. In addition, education programs that focus on the deployment of technology in a privacy-enhancing way should be directed towards agencies and organisations that design and deploy new and developing technologies.[22]

10.18 In Chapter 47, the ALRC discusses the importance of proactive regulation. This is reflected in the recommendations to empower the OPC to conduct 'Privacy Performance Assessments' of organisations, and direct PIAs for new projects and developments of agencies.[23] These recommendations are intended, in part, to promote the early implementation of specific PETs and the deployment of technology in a privacy-enhancing way.

---

19 L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501, 507–510.

20 See, eg, D Post, 'What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace' (2000) 52 *Stanford Law Review* 1439.

21 Rec 10–3.

22 Rec 10–2.

23 See Recs 47–6, 47–4.

Privacy-enhancing technologies

10.19 A number of stakeholders submitted that the ALRC consider the role that PETs could play in a regulatory framework.[24] The term 'PETs' can be used in a number of different contexts. PETs can refer to particular technologies that form part of the architecture of technological systems used by agencies and organisations to deliver services.[25] Chapter 9 includes a discussion of these types of PETs, which may include mandatory access control devices or identity management systems. Secondly, individuals can utilise PETs to exercise control over the collection of their personal information.[26] Several of these types of PETs, including encryption and RFID signal blockers, are discussed in Chapter 9. Finally, the way that technology is used often determines whether its impact is privacy enhancing or invasive.[27] A holistic approach to regulating technology would encourage agencies and organisations to develop and deploy all technologies to enhance privacy, or at least to ensure that their impact is privacy neutral.

10.20 In May 2007, the European Commission issued a communication on PETs to the European Parliament and Council, noting that PETs were most effective when 'applied according to a regulatory framework of enforceable data protection rules'.[28] In the ALRC's view, PETs can promote enhanced security and trust and are, therefore, an essential component of the regulatory structure. Some PETs, however, can be physically unwieldy and costly to implement. Moreover, use of PETs may require a certain level of technological expertise. PETs alone cannot address the impact of technology on privacy and should complement, rather than replace, the legislative and regulatory structure outlined below.

10.21 Use of PETs by individuals—and education about PETs—can provide individuals with greater control over their personal information when using technologies such as the internet. The OPC submitted that:

> Education and PET solutions together will be crucial for dealing with the international nature of the internet and for ensuring that individuals are able to exercise appropriate

---

24 See, eg, Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; CSIRO, *Submission PR 176*, 6 February 2007; Australian Electrical and Electronic Manufacturers' Association, *Submission PR 124*, 15 January 2007; Edentiti, *Submission PR 29*, 3 June 2006.

25 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)*, COM(2007) 228 (2007), 3.

26 Ibid, 3–4.

27 See, eg, J Alhadeff, *Consultation PC 169*, Sydney, 26 April 2007; M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002), 9–10.

28 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)*, COM(2007) 228 (2007), 4.

> control of their personal information when its handling falls outside of the national jurisdiction of Australian privacy law.[29]

10.22 A national survey conducted in May 2007 found that Australians were more concerned about online privacy than the threat of a terrorist attack.[30] PETs, therefore, could play a role in increasing consumer trust in online interactions. Two main types of PETs that may be deployed by individuals to protect their privacy online, encryption and identity management, are discussed in Chapter 9.

10.23 Promoting mechanisms that enhance individual control over personal information is one way to deal with the protection of individual privacy in light of technological developments. Emphasising only the responsibility of individuals to protect their information privacy is undesirable. It places a 'premium' on the individual

> having sufficient interest in protection and the 'cultural capital'—the ability and the means to comprehend what is happening … to read obscure fine print on the web, and to assert herself in controlling inroads or seeking redress once these threats have been realised.[31]

International engagement

10.24 While this chapter focuses on domestic regulation of developing technology, the ALRC notes the jurisdictional issues presented by developing technologies such as the internet. Some of these issues are discussed in Chapter 31.

10.25 In 2006, the United Kingdom Information Commissioner published a report noting that an effective regulator needs to stay 'abreast of, and knowledgeable about, new technologies and systems'.[32] Noting the resource implications, the Commissioner suggested that

> it is advantageous … to develop a pooled technological knowledge-and-awareness capability, as may be occurring, for instance, at the level of the [European Union], through the Article 29 Working Party and other networks and channels in which many national and sub-national regulators participate.[33]

10.26 The OPC expressed its support for 'Australia's involvement in international forums to coordinate data protection schemes'.[34] The Australian Communications and Media Authority (ACMA) suggested that it would be appropriate for both the Australian Government and industry 'to participate in relevant international fora (including technical standardisation discussions) dealing with privacy issues'.[35]

---

29 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
30 Unisys, *Unisys Security Index Australia: A Newspoll Survey May 2007*, 1 May 2007.
31 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, 84.
32 Ibid, 96.
33 Ibid, 96.
34 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
35 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.

10.27 The global nature of technology development and deployment requires industry, the OPC, and the Australian Government to coordinate and engage with others in the international arena. International engagement would also assist the OPC to develop technology-specific guidance on the application of the model UPPs.

10.28 Such international discussions could also consider the impact on privacy of laws such as copyright. For example, Dr Matthew Rimmer submitted that further examination of the intersection between laws that regulate the handling of personal information and laws that prohibit the tampering with technological protection mechanisms (TPMs) is warranted.[36] TPMs, which are discussed further in Chapter 9, have the capacity to collect a significant amount of personal information. As much equipment or media that deploys TPMs is designed in or downloaded from jurisdictions other than Australia, examination of these types of issues at the international level would be worthwhile.

Proactive regulation

10.29 Early regulatory intervention is desirable to prevent interferences with privacy. In Chapter 47, the ALRC recommends that the *Privacy Act* be amended to empower the Privacy Commissioner to conduct Privacy Performance Assessments of the records of organisations for the purpose of ascertaining whether the organisation's records are maintained in compliance with the requirements in the UPPs, privacy regulations and any privacy code that binds the organisation.[37] Further, the ALRC recommends that the OPC should have the power to direct agencies to conduct PIAs for new projects and developments.[38]

10.30 A number of agencies identified the importance of conducting PIAs early in the development of technical systems. The Department of Finance and Deregulation, for example, submitted that:

> The application of PIA process in the initial design and architecture stages identifies possible privacy risks and can lead to innovative and privacy enhancing uses of technology.[39]

10.31 ACMA noted that the PIA conducted for its electronic number mapping (ENUM) project informed its consideration of the impact on privacy of ENUM as well as other new and emerging technologies.[40] ACMA also suggested that PIAs

> can assist in educating individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which these technologies

---

36 M Rimmer, *Submission PR 379*, 5 December 2007.
37 Rec 47–6.
38 Rec 47–4.
39 Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008.
40 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007. ENUM is discussed in Chs 9 and 71.

> can be deployed. The PIA will provide guidance on these issues which in turn can enable the effective dissemination of appropriate educational material to government, industry and consumers.

10.32 In the ALRC's view, the use of Privacy Performance Assessments and PIAs should result in PETs being incorporated into systems and processes, and prevent new or emerging technologies from having an adverse impact on privacy. For example, the 'Anonymity and Pseudonymity' principle in the model UPPs requires agencies and organisations to design systems that allow for anonymous or pseudonymous transactions where it would be practicable to do so. It has been noted that it may not be practicable to alter retrospectively systems such as biometric identification systems or transport systems using smart card technology to allow for anonymity in transactions.[41] PIAs could ensure that agencies and organisations take the impact of technology on privacy into account before a system is developed and, for example, develop systems that provide for anonymous or pseudonymous transactions where appropriate.

Oversight powers of the OPC

Research and monitoring

10.33 The OPC has two research and monitoring functions that are relevant to the regulation of new and developing technologies. These are to:

- conduct research and monitoring into data processing and computer technology (including data-matching and data-linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring;[42] and
- monitor and report on the adequacy of equipment and user safeguards.[43]

Expert panels

10.34 In Chapter 46, the ALRC recommends that the OPC be empowered to convene expert panels to assist with the carrying out of its functions under the *Privacy Act*.[44] In DP 72, the ALRC suggested that such a panel could include experts in information and communication technologies.[45]

---

41 M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

42 *Privacy Act 1988* (Cth) s 27(1)(c). In Ch 47, the ALRC recommends that the first function be amended to remove the word 'computer' to make it clear that the OPC's research and monitoring function is not limited to computer technology: Rec 47–1.

43 Ibid s 27(1)(q). See Ch 47 for a detailed discussion of the existing and proposed powers and functions of the OPC.

44 Rec 46–5.

45 In addition, the OPC is required to include on its Advisory Committee a member with extensive experience in 'electronic data-processing': *Privacy Act 1988* (Cth) s 82(7)(c). In Ch 46, the ALRC proposes that the term 'electronic data-processing' in s 82(7)(c) be replaced with the term 'information and communication technologies': Rec 46–4.

10.35 The Australian Government Attorney-General's Department suggested that any expert panel convened by the OPC should work closely with existing government networks and committees:

> The proposed expert panels appear to be very close to the IT Security Expert Advisory Group of the Trusted Information Sharing Network for Critical Infrastructure Protection. This new proposed panel may also impact upon responsibilities of the E-Security Policy and Coordination (ESPaC) committee chaired by CIP [Criticial Infrastructure Protection] Branch.[46]

10.36 The ALRC agrees that the OPC should be informed by the work of relevant government bodies when carrying out its function to research and monitor information and communication technologies. This process would be complemented by active engagement with international data protection networks. Along with participation in international fora, advice from a range of experts will assist the OPC to carry out its research and monitoring function and other powers and functions relevant to developing technology.

Privacy-enhancing technologies

10.37 In DP 72, the ALRC proposed that, in exercising its research and monitoring functions, the OPC should consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations.[47]

10.38 This proposal was strongly supported.[48] The Office of the Victorian Privacy Commissioner (OVPC) noted the proposal's focus on technology deployment, and submitted that 'the same technology can be either privacy enhancing or extremely privacy intrusive, depending on how it is used: e.g. biometrics smartcards'.[49] The Department of Finance and Deregulation submitted that the use of PETs by agencies is important 'to protect privacy and instil public confidence in government [Information and Communications Technology] services'.[50]

---

46 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–3.

48 See, eg, Unisys, *Submission PR 569*, 12 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

49 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

50 The Department noted that it conducted research into PETs in 2006 and suggested that it could assist the OPC in researching and promoting the use of PETs by agencies: Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 2008.

10.39 The Cyberspace Law and Policy Centre was concerned that the ALRC's proposal did not address privacy-invasive technologies. The Centre also submitted that:

> The Office of the Privacy Commissioner should pay special attention to technologies that appear to be privacy enhancing, however only offer minimal protection. For example, 'privacy seals' have been used as an example of technology utilised mainly to offer the illusion of privacy rather than true privacy protection. The Platform for Privacy Preferences (P3P) was also once lauded as a PET, but has been criticised widely and does not seem to have advanced.[51]

10.40 The ALRC notes that the OPC is already required by the *Privacy Act* to research and monitor technological developments to ensure that any adverse effects of such developments on the privacy of individuals are minimised.[52] This requires research into and monitoring of privacy-invasive technologies, and technologies that may be used in a privacy-invasive way.[53]

10.41 In the ALRC's view, in addition to considering technologies that have an adverse impact on privacy, the OPC should consider PETs when exercising its research and monitoring function. In particular, the function to research and monitor user safeguards could be relied on to support research on PETs such as online authentication and identity management systems. In exercising this function, the OPC should consult with experts and other relevant stakeholders. The OPC should also be aware that the privacy-enhancing aspects of some technologies may be overstated, and that frequently it is the way in which technology is deployed that determines whether it is privacy enhancing or invasive.

Recommendation 10–1 In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations.

Education

10.42 The OPC is also required to undertake and coordinate educational programs for the purposes of promoting individual privacy.[54] In DP 72, the ALRC noted that the technical expertise attained by the OPC in exercising its research and monitoring functions could form the basis of educational programs. The ALRC proposed that the OPC should educate individuals, agencies and organisations about specific privacy-enhancing technologies and the privacy-enhancing ways in which technologies can be deployed.[55]

---

51 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
52 *Privacy Act 1988* (Cth) s 27(1)(c).
53 The impact on privacy of several technologies is discussed further in Ch 9.
54 *Privacy Act 1988* (Cth) s 27(1)(m).
55 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–4.

Submissions and consultations

10.43 Some stakeholders supported this proposal.[56] The Cyberspace Law and Policy Centre suggested that the OPC should also educate individuals, agencies and organisations about 'PETs that only provide a minimal degree of privacy protection'.[57]

10.44 The OVPC submitted that, to ensure national consistency, the proposed education programs should be conducted in consultation with Privacy Commissioners in other jurisdictions.[58] It also submitted that, when conducting education programs, 'care should be taken to preserve against seeming to endorse specific products and manufacturers'.[59]

10.45 Some stakeholders noted that education programs on privacy and information security are already conducted by agencies. The Australian Government Department of Broadband, Communications and the Digital Economy stated that the Stay Smart Online website 'provides information to home and small business users on how to improve their security, and subsequently their privacy, when online'.[60] The Attorney-General's Department noted the overlap between privacy and information security, and expressed concern that the implementation of the ALRC's proposal would require significant resources and duplicate work.[61]

ALRC's view

10.46 The OPC and relevant stakeholders should conduct education programs which focus on specific, useful PETs and the privacy-enhancing ways in which technologies can be deployed. Such education programs should be directed towards those designing technical systems; agencies and organisations that use the systems to deliver services; and individuals that use such systems.

---

56 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 Government Department of Human Services, *Submission PR 541*, 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; Australasian Compliance Institute, *Submission PR 419*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

58 In Ch 17, the ALRC recommends that, when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies that handle personal information, the Australian Government agency should ensure that a memorandum of understanding or other arrangement is in place to ensure appropriate handling of personal information: Rec 17–1.

59 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

61 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

10.47 Appropriate consultation between the OPC and other agencies will avoid the problems of duplication of work highlighted by the Attorney-General's Department. Awareness by the OPC of relevant education programs conducted by other agencies is necessary to ensure that resources are used in a targeted and efficient way.

10.48 The ALRC also recommends that, to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy and, in particular, privacy in the online environment, into school curricula.[62]

Recommendation 10–2 The Office of the Privacy Commissioner should develop and publish educational materials for individuals, agencies and organisations about specific privacy-enhancing technologies and the privacy-enhancing ways in which technologies can be deployed.

Technology-specific guidance on the application of the model UPPs

10.49 In IP 31, the ALRC asked whether the privacy principles should be amended to deal with the impact of developing technology on privacy.[63] In DP 72, the ALRC expressed the view that these issues should not be covered in the model UPPs, but instead could form the subject of technology-specific guidance.

10.50 As noted at the beginning of this chapter, to operate effectively, principles-based and compliance-oriented regulatory schemes require the issuing of non-binding guidance that clarifies the rights and obligations contained in the primary legislation.[64] In Chapter 9 the ALRC examines a number of developing technologies that may require such guidance when used by agencies and organisations to handle personal information.[65] For example, RFID systems, surveillance devices and internet software could allow an agency or organisation to collect personal information about an individual without his or her knowledge or consent. Security issues may arise when information is transmitted by wireless technologies, and large quantities of information are stored electronically. It may also be difficult for an individual to gain meaningful access to personal information that an organisation holds in an encrypted form.

---

62 See Rec 67–3. In Ch 67, the ALRC discusses different attitudes to privacy held by members of different generations.

63 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.125]–[11.140].

64 See also Chs 4, 18.

65 In Ch 71, the ALRC recommends that ACMA, in consultation with the OPC, Communications Alliance, the Telecommunications Industry Ombudsman, and other relevant stakeholders, should develop and publish guidance that addresses privacy issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping: Rec 71–4.

10.51 Agencies and organisations using such technologies to handle an individual's personal information may be required to do certain things to meet the obligations set out in the model UPPs. Guidance issued by the OPC—for example, technology-specific guidelines—could specify what is required to fulfil the obligations in the UPPs when personal information is handled using a particular technology.

10.52 The OPC has the power to prepare guidelines that assist agencies and organisations to avoid acts or practices that may be interferences with, or adversely affect, the privacy of individuals.[66] The OPC has used this power to issue guidelines that deal with the data-matching activities of agencies.[67] While guidelines such as these are not binding, they indicate the OPC's understanding of the requirements set out in the privacy principles. Guidelines can provide greater detail than high level principles, and help to modify behaviour. They can also be highly persuasive in the complaint-handling process. The OPC may also take into account compliance with guidelines when conducting an audit or Privacy Performance Assessment.[68]

10.53 In formulating guidance, the OPC could examine similar guidance published in other jurisdictions. For example, in June 2006, the Information and Privacy Commissioner Ontario issued *Privacy Guidelines for RFID Systems*. These guidelines are not mandatory, but encourage agencies and organisations to comply with certain limits on collection, use and disclosure of information collected by RFID tags embedded in retail items.[69] In January 2008, the United Kingdom Information Commissioner's Office published an updated CCTV code of practice.[70] The non-binding code provides advice about how agencies and organisations that use CCTV or similar devices can meet the requirements in the *Data Protection Act 1998* (UK).

Collection

10.54 The 'Collection' principle requires an agency or organisation to collect information only by fair means, and not in an unreasonably intrusive way.[71] In DP 72, the ALRC proposed that guidance issued by the OPC could explain the meaning of the terms 'fair means' and 'unreasonably intrusive' in relation to certain technologies.[72] This may be required where technologies allow the collection of information without the knowledge of an individual.

---

66 This power is discussed in Ch 47.

67 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998).

68 Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 5. In Ch 47, 'Privacy Performance Assessments' are recommended: Rec 47–6.

69 Information and Privacy Commissioner of Ontario, *Privacy Guidelines for RFID Information Systems* (2006).

70 United Kingdom Government Information Commissioner's Office, *CCTV Code of Practice—Revised Edition* (2008).

71 See the 'Collection' principle set out in the model UPPs.

72 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–5(a).

10.55 In DP 72, the ALRC provided examples of situations that the OPC could consider in formulating this guidance. The ALRC suggested that an unreasonably intrusive collection of information by RFID systems might involve collection of information from an RFID tag combined with a location detection sensor embedded in an item of clothing sold by a retailer. The ALRC also suggested that collection of information by keystroke software installed on internet cafe computers may not fall within the definition of 'fair means'.

10.56 This proposal—and most of the proposals relating to technology-specific guidance—received general support from stakeholders.[73] The Department of Human Services indicated that the proposed guidance would be a cost-effective way to raise awareness of individual rights, educate agencies and organisations about their privacy obligations with respect to developing technology, and facilitate compliance with the Act.[74]

10.57 The OVPC submitted that the proposals relating to guidance should be produced jointly with Privacy Commissioners in all Australian jurisdictions and 'should be applicable to the federal public sector, the private sector and to state and territory public sectors'.[75]

10.58 The Communications Alliance Ltd submitted that the OPC guidance should be developed in consultation with the communications industry.[76] ACMA observed that the development of appropriate guidance for new and emerging technologies also will require ongoing Australian involvement in international standard-making forums, and OPC liaision with relevant agencies.

10.59 ACMA also suggested that the PIA process

> could be used as part of guidance provided by [the] OPC to describe and de-mystify the particular technology in question; identify and analyse possible privacy implications; make recommendations for minimising privacy intrusion and maximising privacy protections, while ensuring that the objectives associated with the proposed deployment and use of the technology are met.[77]

10.60 In the ALRC's view, the OPC should issue guidance on what agencies and organisations need to do to meet the requirements in the 'Collection' principle when using technologies, such as RFID and biometric systems, to handle personal information. This guidance should provide examples, such as when the use of a certain

---

73 See, eg, Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007.

74 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

75 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. See Rec 17–3.

76 Communications Alliance Ltd, *Submission PR 439*, 10 December 2007.

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

technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way'.

Notification

10.61 In response to IP 31, the ALRC received limited support for requiring agencies and organisations that use certain technologies to collect personal information to comply with additional notice requirements. In DP 72, the ALRC stated that including such requirements in the 'Notification' principle would not be consistent with its high-level, technology-neutral approach. The ALRC proposed that this issue could form one subject of technology-specific guidance on the 'Notification' principle.[78]

10.62 The ALRC provided a non-exhaustive list of what could be included in such guidance. For example, guidance on RFID could encourage agencies and organisations to inform an individual about how to remove or deactivate an RFID tag embedded in a product. Agencies and organisations using biometric systems could be required to inform individuals of the error rates of the systems, and the steps that can be taken by an individual wishing to challenge the system's results.[79] Further, guidance could encourage agencies or organisations to inform individuals of the format in which personal information may be disclosed—for example, whether it will be disclosed in an electronic format.

10.63 The OPC stated that 'technology-specific notice requirements are likely to be prescriptive and therefore at odds with the concept of principles-based law'. The OPC submitted that, instead, 'requirements for new technologies should be incorporated in technologically specific binding guidelines and industry codes'.[80]

10.64 In the ALRC's view, the OPC should issue guidance that clarifies the requirements under the 'Notification' principle when personal information is handled by new and emerging technologies. This recommendation is consistent with the ALRC's regulatory approach set out at the beginning of this chapter and in Chapter 4. It is also consistent with the other recommendations in this section.

10.65 In addition, if a particular technology requires more stringent notification requirements, these could be included in a technology-specific privacy code approved by the OPC and made mandatory under Part IIIAA of the *Privacy Act*.[81] The OPC could also initiate its own code for the handling of personal information by a particular

78 Australian Law Reform Commission, Review of Australian Privacy Law, DP 72 (2007), Proposal 7–5(b).
79 See Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), 11.
80 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
81 Codes are discussed further in Ch 48.

technology, and lobby the minister responsible for administering the *Privacy Act* to have this promulgated by regulations.[82]

Data security

10.66 The 'Data Security' principle in the model UPPs requires agencies and organisations to take reasonable steps to protect personal information from loss, misuse and unauthorised access, modification or disclosure. In relation to the IPPs and the NPPs that deal with data security, the OPC has indicated that 'reasonable steps' will depend on: the sensitivity of the personal information held; the circumstances in which the personal information is held; the risks of unauthorised access to the personal information; the consequences to the individual of unauthorised access; and the costs of security systems.[83]

10.67 In Chapter 28, the ALRC recommends that the OPC provide guidance on the meaning of the term 'reasonable steps' in the 'Data Security' principle. This guidance should refer to technological developments in this area and, in particular, relevant encryption standards.[84] In addition, the ALRC recommends that the OPC provide guidance on what is required of an agency or organisation to destroy or render non-identifiable personal information, particularly when that information is held or stored in an electronic form.[85]

Access and correction

10.68 The 'Access and Correction' principle provides individuals with a general right to access personal information about them that is held by agencies and organisations.[86] In IP 31, the ALRC noted that some personal information may be stored in a way that makes it difficult to analyse or comprehend.[87] The European Parliament *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) requires personal information to be communicated to an individual in an 'intelligible form'.[88] This could mean, for example, that a machine capable of reading biometric information, or an expert with the ability to interpret the results of a machine's analysis of biometric information, should be made available to an individual seeking to exercise his or her right of access to this type of personal information.[89]

---

82 The regulation-making power is discussed in Ch 5.

83 *Privacy Act 1988* (Cth) s 14, IPP 4; sch 3, NPP 4.1; Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001), 1.

84 Rec 28–3.

85 Rec 28–4.

86 See Ch 29.

87 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.132].

88 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(a).

89 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [82].

10.69 In DP 72, the ALRC suggested that it is implicit in the 'Access and Correction' principle that, where an individual requests access to personal information about him or her that is held by an organisation, the organisation should provide access to the information in an intelligible form where this is practicable. Moreover, the ALRC noted that it is best practice for organisations to hold some information only in encrypted form. For example, the sensitive nature of biometric information—and the difficulty of replacing such information if it is compromised—means that an organisation should generally destroy the raw data, such as digital photographs, that are obtained when an individual enrols in a biometric system.[90] The ALRC proposed that the OPC should provide guidance on the type of information that an agency or organisation should make available to an individual when information is held in an encrypted form.[91]

10.70 In its response to DP 72, the OPC disagreed with the ALRC's view that the proposed 'Access and Correction' principle necessarily implied that access to personal information be provided in an intelligible form where this is practicable.

> This Office believes that a change which allowed for information to be presented in a comprehensible form would enhance individuals' access rights. The Office is aware that there will be occasions where it may be extremely difficult for information to be presented in an intelligible form. For this reason, the Office submits that personal information should be made accessible in an intelligible form where practicable.[92]

ALRC's view

10.71 There is no evidence to indicate that agencies and organisations are providing information to individuals in an unintelligible form. It is implicit in the 'Access and Correction' principle that, where an individual requests access to personal information about him or her that is held by an agency or organisation, the agency or organisation should provide access to the information in an intelligible form, where this is practicable. Section 25A of the *Acts Interpretation Act 1901* (Cth) states that, where a person is required by or under an Act to make available to a court, tribunal or person, information that is kept in a mechanical, electronic or other device, that information should be reproduced in a form capable of being understood by the court, tribunal or person. This provision appears applicable to individuals' rights of access under the *Privacy Act*.

10.72 The ALRC is also concerned that drafting the 'Access and Correction' principle in line with the OPC's submission could have unintended consequences. Requiring agencies and organisations to provide an individual with information held about them in an intelligible form may encourage organisations to hold certain information, which

---

90 See, eg, Biometrics Institute, *Biometrics Institute Privacy Code* (2006), Principle 11.

91 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–5(d).

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

for security reasons should be encrypted permanently, in an unencrypted form or a form that is able to be decrypted.

10.73 On balance, therefore, the 'Access and Correction' principle should not be drafted to provide individuals with a right to access information in an intelligible form. The OPC should provide guidance on the type of information that an agency or organisation should make available to an individual when information is held in an encrypted form. This could include, for example, information about whether an encrypted biometric template is a facial or fingerprint biometric.

10.74 The 'Access and Correction' principle requires an agency and an organisation to take reasonable steps to correct personal information about an individual when that individual establishes that information held by the agency or organisation is not accurate, complete, up-to-date or relevant.[93] For example, if an organisation's biometric system repeatedly fails to identify or authenticate an individual who had provided the organisation with biometric information to enrol in the system, this indicates that the biometric information held by the organisation is not accurate, complete or up-to-date. In this context, it would be reasonable for the organisation to re-enrol that individual in the biometric system.[94]

Automated decision review mechanisms

10.75 Article 15(1) of the EU Directive reflects concern about the increasing automation of decisions that affect individuals.[95] It states:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[96]

10.76 In the United Kingdom, a data controller, on request in writing by an individual, is required 'to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data'.[97]

---

93 See Ch 29.

94 Biometric systems are discussed in detail in Ch 9.

95 L Bygrave, 'Minding the Machine: Art 15 of the EC Data Protection Directive and Automated Profiling' (2000) 7 *Privacy Law & Policy Reporter* 67, 68.

96 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 15(1). The United Nations Human Rights Committee has also stated that art 17 of the *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976) means that an individual has the right to 'ascertain in an intelligible form' personal data that is stored in automatic data files: United Nations Office of the High Commissioner for Human Rights, *General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art 17)* (1988), [10].

97 *Data Protection Act 1998* (UK) s 12(1).

10.77 In 2004, the Administrative Review Council (ARC) published a report that contained a number of principles for agencies carrying out automated decision-making processes, and included a principle that provided for the manual review of decisions in certain circumstances.[98] The ARC Report was the basis for a guide published in February 2007 by the Australian Government Information Management Office (AGIMO).[99] This guide provides suggestions on when automated systems may be suitable for administrative decision making, the development and governance of automated systems and the design of such systems.

10.78 Research into computer systems indicates that such systems are not inherently accurate and reliable. Dr Cameron Spenceley notes that the reliability of computer hardware 'is governed not only by the validity and integrity of its design, but also by the lifespan of its physical components'.[100] Further, Spenceley states that the 'proposition that the reliability of computer software generally meets or exceeds some threshold is not demonstrable on an inherent or empirical basis with information and data that are generally available'.[101]

10.79 In IP 31, the ALRC asked whether an additional privacy principle for automated decision-making processes was required. In DP 72, the ALRC proposed that human review of automated decision-making processes should be the subject of guidance issued by the OPC.[102] The ALRC suggested that such guidance could be based on the material on automated decision-making processes produced by the ARC and AGIMO.

Submissions and consultations

10.80 In response to DP 72, some stakeholders supported the inclusion in the 'Data Quality' principle of a requirement for the review of automated decisions. The OPC was concerned that the ALRC's proposal would be 'a reiteration of the ARC's guidelines rather than an enforceable mechanism'. The OPC submitted that the 'Data Quality' principle should be amended to include a technology-neutral review mechanism.[103]

---

98 Administrative Review Council, *Automated Assistance in Administrative Decision Making*, ARC 46 (2004), Principle 22.

99 Australian Government Information Management Office, *Automated Assistance in Administrative Decision-Making Better Practice Guide* (2007).

100 C Spenceley, 'Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation', *Thesis*, University of Sydney, 2003, 121.

101 Ibid, 151.

102 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–5(e).

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

10.81 The Cyberspace Law and Policy Centre stated that

> the proposed 'Data Quality' principle (though not the 'Access and Correction' principle) in the UPPs could be taken to impose such a requirement in some circumstances, but submits that it should be made an express requirement as part of UPP 7, with an appropriate 'reasonable steps' limitation.[104]

10.82 ANZ submitted that it had considerable experience in using automated decision-making models to assess applications for products such as credit cards and personal loans. ANZ stated that 'well designed models do not produce inaccurate or unreliable results and have not generated consumer dissatisfaction'.[105]

ALRC's view

10.83 Ensuring that accurate decisions are made about individuals is in the interests of the agencies and organisations that make such decisions. The ALRC supports the practice of human review of decisions that are made by automated means, particularly when an agency or organisation plans to take adverse action against an individual on the basis of such a decision. In supporting this practice, the ALRC notes research that indicates that computer software and hardware may not necessarily produce accurate and reliable results.

10.84 The ALRC, however, received no concrete example of harm resulting from automated decision making by agencies and organisations. This indicates that the inclusion in the 'Data Quality' principle of a prescriptive requirement for human review of automated decisions is not required. 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. In light of a demonstrated lack of harm, guidance should address the issue appropriately.

10.85 The model UPPs generally provide high-level and outcomes-based requirements.[106] The 'Data Quality' principle requires an agency or organisation to take reasonable steps to make sure that personal information that it collects, uses or discloses is accurate, complete, up-to-date and relevant. This principle provides for outcomes relevant to review of decisions made by automated means.

Data-matching

10.86 Data-matching is 'the large scale comparison of records or files … collected or held for different purposes, with a view to identifying matters of interest'.[107] Privacy concerns about data-matching include the: revealing of previously unknown information about an individual without the knowledge or consent of that individual;

---

104 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
105 ANZ, *Submission PR 467*, 13 December 2007.
106 See Chs 4, 18.
107 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [14].

profiling of an individual; difficulty for an individual in accessing information contained in the new data-set without knowledge that such a data-set was compiled; accuracy of the matched data; and security of large amounts of data collected for the purposes of data-matching or data mining.[108]

Regulation of data-matching

10.87 Currently, agencies that conduct data-matching activities are subject to regulation additional to the privacy principles. Mandatory rules apply to data-matching involving tax file numbers[109] and the OPC has published guidance that applies to other data-matching activities of agencies.[110] Data-matching conducted by organisations may be subject to some of the privacy principles, but there is no specific regulation of the data-matching activities of organisations. This section considers whether greater regulation of data-matching activities is required.

10.88 The Privacy Commissioner has functions relating to data-matching. These include undertaking research and monitoring developments in data processing and computer technology (including data-matching and data linkage) to help minimise any adverse effects of such developments on privacy.[111] In addition, the Privacy Commissioner can examine (with or without a request from a minister) any proposal for data-matching or data linkage that may involve an interference with privacy or that may have any adverse effects on the privacy of individuals.[112] The Privacy Commissioner may report to the minister responsible for administering the *Privacy Act*[113] about the results of any research into developments in data-matching or proposals for data-matching.[114]

10.89 The *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the *Data-matching Program (Assistance and Tax) Guidelines* (the Guidelines) regulate the use of tax file numbers to match data held by certain agencies, such as the Australian Taxation Office and Centrelink.[115] The Privacy Commissioner monitors compliance with the Act and the Guidelines. The Privacy Commissioner advises agencies about the interpretation of the Act and inspects the way in which they undertake data-matching

---

108 The impact on privacy of data-matching is discussed further in Ch 9.

109 *Data-matching Program (Assistance and Tax) Act 1990* (Cth); Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997).

110 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998) <www.privacy.gov.au> at 5 May 2008.

111 See *Privacy Act 1988* (Cth) s 27(1)(c).

112 Ibid s 27(1)(k).

113 Commonwealth of Australia, *Administrative Arrangements Order*, 25 January 2008 [as amended 1 May 2008].

114 *Privacy Act 1988* (Cth) ss 27(1)(c), 32(1).

115 See Ch 9.

regulated by the Act.[116] An act or practice that breaches Part 2 of the *Data-matching Program (Assistance and Tax) Act*, or the Guidelines, constitutes an 'interference with privacy'.[117] An individual can complain to the Privacy Commissioner about any such act or practice.[118]

10.90 Agencies may also engage in data-matching activities that do not involve the use of tax file numbers. For example, in early 2004, the Australian Securities and Investments Commission (ASIC) began matching data from its public database with data from the Insolvency and Trustee Service Australia's National Personal Insolvency Index.[119] The purpose of this data-matching program is to identify individuals who should be disqualified automatically from managing corporations under the *Corporations Act 2001* (Cth).[120]

10.91 The Privacy Commissioner has issued guidelines for agencies that engage in data-matching practices that are not regulated by the *Data-matching (Assistance and Tax) Act 1990* (Cth) (the voluntary data matching guidelines).[121] The voluntary data-matching guidelines aim to ensure that data-matching programs 'are designed and conducted in accordance with sound privacy practices'.[122] Although the guidelines are not legally binding, a number of agencies have agreed to comply with them.[123]

10.92 The voluntary data-matching guidelines apply to agencies that match data from two or more databases, if at least two of the databases contain information about more than 5,000 individuals.[124] In summary, the guidelines require agencies to: give public notice of any proposed data-matching program; prepare and publish a 'program protocol' outlining the nature and scope of a data-matching program; provide individuals with an opportunity to comment on matched information if the agency proposes to take administrative action on the basis of it; and destroy personal information that does not lead to a match. Further, the voluntary data-matching guidelines generally prohibit agencies from creating new, separate databases from information about individuals whose records have been matched.[125]

---

116 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), [3.8].
117 *Privacy Act 1988* (Cth) s 13.
118 Ibid s 36; *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 14.
119 Australian Securities and Investments Commission, *ITSA Data Matching Protocol* <www.asic.gov.au> at 1 May 2008.
120 Ibid.
121 Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997).
122 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), 1.
123 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 68–71.
124 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [15].
125 Ibid, [33]–[41], [42]–[47], [63], [69].

Submissions and consultations

10.93 In IP 31, the ALRC asked whether data-matching programs that fall outside the *Data-matching Program Assistance and Tax Act* should be regulated more formally.[126] In DP 72, the ALRC proposed that the OPC should issue guidance that applies to data-matching by organisations.[127] The ALRC suggested that this guidance could be in the form of guidelines that are based on the existing data-matching guidelines that apply to agencies.

10.94 A number of stakeholders submitted that the privacy principles do not regulate adequately the data-matching activities of organisations.[128] Centrelink supported the ALRC's proposal, noting that the proposed guidance 'would enhance the privacy of citizens and make processes consistent across agencies and organisations'.[129] The OPC submitted that it 'is committed to issuing guidelines on best practice for data-matching activities'.[130]

10.95 Other stakeholders expressed concern that the ALRC's proposal fell short of providing adequate privacy protection for data-matching activities conducted by organisations. The OVPC supported the introduction into the *Privacy Act* of statutory provisions modelled on Part X of the *Privacy Act 1993* (NZ)—which provides regulation of information-matching programs conducted by New Zealand agencies.[131] The Office of the Privacy Commissioner submitted that it be empowered to make binding codes for data-matching activities undertaken by specific industries.[132]

10.96 Several stakeholders stated that agencies should be subject to greater regulation when conducting data-matching programs.[133] The OPC submitted that the existing voluntary data-matching guidelines should be reviewed and made mandatory.[134]

---

126 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(h).

127 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–6.

128 See, eg, Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 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.

129 Australian Government Centrelink, *Submission PR 555*, 21 December 2007. See also National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

131 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

133 See, eg, Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Australian Privacy Foundation, Submission PR 167, 2 February 2007.

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

ALRC's view

10.97 While several stakeholders expressed concern about the privacy implications of data-matching activities, there is no indication that agencies are not currently complying with the voluntary data-matching guidelines issued by the OPC. A case has not been made out, therefore, for making these guidelines mandatory. In reaching this decision, the ALRC notes that one of the functions of the OPC, discussed above, is to research and monitor technology, including data-matching, and report the results to the minister. The OPC could exercise this function to review the adequacy of, and compliance with, the existing guidelines if the OPC deems this to be necessary.

10.98 In Chapter 5, the ALRC 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 on agencies and organisations.[135] This mechanism could be used to provide greater regulation of the data-matching activities of agencies and organisations if the minister responsible for administering the *Privacy Act* deems this to be necessary. If the OPC finds that agencies are not complying with the voluntary data-matching guidelines, the OPC can lobby the relevant minister to have more stringent regulation of data-matching promulgated by regulation.

10.99 A similar staged approach could be followed for the regulation of data-matching activities conducted by organisations. There is currently no OPC guidance that applies to organisations engaged in data-matching. The OPC should develop and publish guidance for organisations on the privacy implications of data-matching. This guidance could be in the form of guidelines that are based on the existing data-matching guidelines that apply to agencies. If this guidance is found to be inadequate, the OPC could lobby the relevant minister to introduce regulations.

Recommendation 10–3 The Office of the Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy. This guidance should incorporate relevant local and international standards. Matters that such guidance should address include:

(a) developing technologies such as radio frequency identification (RFID) or data-collecting software such as 'cookies';

(b) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';

(c) when the use of a certain technology will require agencies and organisations to notify individuals at or before the time of collection of personal information;

135 Rec 5–1.

(d) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometric systems);

(e) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information in an intelligible form (for example, the type of biometric information that is held as a biometric template); and

(f) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.

Recommendation 10–4 The Office of the Privacy Commissioner should develop and publish guidance for organisations on the privacy implications of data-matching.

Mandating standards?

10.100 The term 'standardisation' can be used to refer to consistency and interoperability between technical systems. Standards also require compliance with certain specifications and procedures that are intended to result in appropriate levels of safety, privacy or security.[136]

10.101 Local and international bodies are continuing to develop standards on privacy and security issues such as identification, authentication and encryption. There may not be adequate incentive for agencies and organisations to comply with standards, however, because of a lack of adequate enforcement mechanisms. For example, it was noted recently that 83% of large merchants using Visa are not in compliance with the Payment Card Industry (PCI) Data Security Standard.[137] In addition, a proliferation of local and international standards for technologies such as voice over internet protocol (VoIP) and RFID can result in inconsistent privacy and security protection for individuals.

136 It has been noted that information security is increasingly relevant to privacy: P Cullen, T Hughes and M Crompton, *Consultation PC 19*, Sydney, 8 May 2006.

137 D Rosenblum, 'Achieving PCI Compliance with Storage Security Systems' (2007) (1) *Computer Technology Review* <www.wwpi.com>.

10.102 In DP 72, the ALRC proposed that the *Privacy Act* be amended to empower the minister responsible for the *Privacy Act*, in consultation with the OPC, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.[138]

10.103 In making this proposal, the ALRC's intention was to promote the incorporation of security mechanisms and PETs in the design stage of technical systems. Empowering the minister to determine relevant standards would not require the listing of privacy and security standards in the *Privacy Act*. Rather, the proposal would provide the minister with the discretion to mandate in regulations certain standards where he or she considered this to be appropriate.

Submissions and consultations

10.104 There was some support for this proposal.[139] Most stakeholders, however, opposed it. Stakeholders expressed concern that technical standards could quickly become outdated.[140] The Department of Human Services submitted the proposed regulations would 'constrain business improvement at a time when technology is rapidly changing'.[141] The Defence Signals Directorate suggested that a better instrument for determining privacy and security standards might be the regularly updated *Australian Government Information Technology Security Manual* (ACSI 33).[142]

10.105 Stakeholders were also concerned about the impact of the ALRC's proposal on Australia's technology industry. The Attorney-General's Department noted that Australia plays a minor role in the global economy. The Department suggested that onerous regulation of security standards may impact negatively on the development of technical systems in Australia and make many globally-developed technical systems and products unavailable for use in Australia.[143] ACMA also submitted that the implementation of this proposal would require the Australian Government to consider its obligations under relevant free trade agreements and rules issued by the World Trade Organization.[144]

---

138 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 7–2.

139 See, eg, 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.

140 See, eg, Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007.

141 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

142 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466*, 13 December 2007.

143 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007. See also BPay, *Submission PR 566*, 31 January 2008; Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007.

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

10.106 Other stakeholders agreed with the policy underpinning the proposal, but expressed concern about its operation. For example, the OPC submitted that mandating standards 'might in some circumstances be consistent with the multi-faceted approach to protecting privacy in the context of new technologies'. Before it could support the proposal, however, the OPC indicated that it would require clarification and additional information on aspects of the scheme, such as monitoring and enforcing compliance.[145]

10.107 The Government of South Australia expressed concern that mandating standards in Australian Government regulations would lead to fragmentation and inconsistency for state and territory jurisdictions.[146]

ALRC's view

10.108 Mandating standards in regulations could have unintended consequences in the face of rapid technological development. The proposed standards-making mechanism is likely to be too inflexible, with the regulations fast becoming outdated. Compliance with the proposed regulations is also likely to impact negatively on the availability of technical systems in Australia.

10.109 The ALRC remains committed to the policy goal of ensuring that privacy and security safeguards are incorporated into systems design. The early incorporation of privacy and security safeguards in technical systems is fundamental for the optimal protection of personal information handled by these systems.

10.110 In DP 72, the ALRC provided an overview of relevant privacy and security standards made by domestic and international standards-making bodies.[147] The ALRC also notes that ACSI 33 provides a useful reference for determining relevant privacy and security standards. The OPC, in carrying out its functions under the *Privacy Act*, should refer to the work of agencies such as the Defence Signals Directorate and national and international standards bodies. In particular, the OPC should play a proactive role in educating and providing guidance to those designing technical systems about the importance of complying with relevant standards in the design of those systems.

10.111 Relevant standards issued by national and international bodies also should be an essential consideration in the PIA process. As discussed above, PIAs are an important proactive mechanism through which to ensure that privacy and security safeguards are taken into account in the development of new projects.

---

145 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
146 Government of South Australia, *Submission PR 565*, 29 January 2008.
147 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [7.58]–[7.63].

Co-regulation between the OPC and industry

10.112 The *Privacy Act* currently provides, through the OPC's power to approve privacy codes, a form of co-regulation for organisations that develop and deploy particular technologies.[148] Once a privacy code has been developed by an industry and approved by the OPC, the requirements set out in the code are binding on organisations that have agreed to be bound.[149]

10.113 At several points throughout this chapter, the ALRC has noted where the code-making mechanism could provide additional privacy protection of personal information handled by an agency or organisation using a particular technology. Two technology-specific codes are the Biometrics Institute Privacy Code and the Internet Industry Association Draft Code. A detailed discussion of these two codes can be found in DP 72[150] and on the websites of the organisations.[151]

Technology-related amendments to the *Privacy Act*

10.114 This section focuses on the amendments to the *Privacy Act* that the ALRC recommends to ensure that the Act remains technology aware. In this section, recommended content of the model UPPs and the definitions relevant to technology are discussed.

The model UPPs

10.115 The model UPPs are intended to regulate personal information throughout the information-handling cycle. In formulating the UPPs, the ALRC addressed developments in technology by recommending several additions and amendments to the existing wording in the NPPs and IPPs. Part D contains a detailed examination of each UPP.

Anonymity and pseudonymity

10.116 In Chapter 20, the ALRC recommends that the privacy principle dealing with anonymity should also include a pseudonymity requirement that states that, when an individual is interacting with an agency or organisation, the agency or organisation must give the individual, where providing this option is lawful and practicable, the clear option of identifying themselves by a pseudonym.[152] Having the option to interact anonymously provides an individual with control over what information is collected about them by an agency or organisation, particularly in an electronic environment. It may not always be practicable, however, for an agency or organisation to interact anonymously with individuals. In these circumstances it may be practicable for an

148 *Privacy Act 1988* (Cth) pt IIIAA.

149 Further discussion of the operation of the current code-making power and the co-regulatory nature of privacy codes is contained in Ch 48.

150 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [7.127]–[7.132].

151 Biometrics Institute, *Biometrics Institute Ltd* <www.biometricsinstitute.org> at 5 May 2008; Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001).

152 Rec 21–1.

individual to interact with an agency or organisation using a privacy-enhancing pseudonym.

10.117 The 'Anonymity and Pseuonymity' principle is the first listed principle in the UPPs. It reflects

> the idea that the lifecycle of information begins before collection, when organisations and agencies should consider the fundamental question of whether they need to collect personal information at all.[153]

Collection

10.118 In Chapter 21, the ALRC recommends that the 'Collection' principle in the model UPPs should provide that, where an agency or organisation receives unsolicited personal information, it must either: 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 comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.[154] This recommendation provides a mechanism for dealing with circumstances when an agency or organisation might inadvertently collect information—for example, when information passes over a system electronically.

10.119 The *Privacy Act* does not require agencies or organisations to obtain an individual's consent before collecting non-sensitive personal information. Sensitive information is subject to greater restrictions and consent generally is required for collection. In IP 31, the ALRC asked whether there are categories of personal information that can be collected by new technologies that should only be collected with consent.[155] Some stakeholders submitted that consent should be obtained before the collection of information by RFID or biometric systems.[156] Several stakeholders, however, opposed the introduction into the 'Collection' principle of a requirement that an agency or organisation needs to obtain consent prior to the collection of personal information by certain technologies. They argued that such a requirement would be inconsistent with the technological neutrality of the *Privacy Act*.[157]

---

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

154 Rec 21–3.

155 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.126].

156 Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

157 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007.

10.120 The OPC submitted that another approach may be to 'increase protections for particular types of information rather than particular types of technology'.[158] The ALRC agrees with this approach. In Chapter 6, the ALRC recommends that biometric information, collected for certain purposes, should be included in the definition of sensitive information.[159]

Notification

10.121 Technologies such as RFID, optical surveillance devices and computer software can allow the collection of information about an individual from that individual without his or her knowledge.[160]

10.122 In Chapter 23, the ALRC recommends that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of, amongst other things, the fact and circumstances of collection where the individual may not be aware that his or her personal information has been collected—for example, how, when and from where the information was collected.[161] This will provide the individual with the knowledge that his or her information has been collected, and some understanding of how technology was used to collect it.

Identifiers

10.123 In Chapter 30, the ALRC notes that agencies increasingly use biometric information, including facial images, iris scans and fingerprints, as identifiers. The ALRC recommends, therefore, an amended definition of 'identifier' in the 'Identifiers' principle. The amended definition will make it clear that the definition includes biometric information that is collected for the purpose of automated identification or verification of identity.[162]

Data breach notification

10.124 In Chapter 51, the ALRC recommends that the *Privacy Act* be amended to include a new Part on data breach notification.[163] Breaches of data security are particularly relevant in the context of developing technology, given that technologies such as the internet can provide a vehicle for the widespread dissemination of personal information.

---

158 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
159 Rec 6–4.
160 Developing technologies are discussed in Ch 9.
161 Rec 23–2.
162 Rec 30–3.
163 Rec 51–1.

10.125 Generally, an agency or organisation would be required to notify the Privacy Commissioner and affected individuals when a data breach occurs that may give rise to a real risk of serious harm to any affected individual.[164]

Definitions in the *Privacy Act*

10.126 This section outlines the recommended amendments to definitions of terms in the *Privacy Act* that are relevant to technology. Detailed discussion of the following amendments is contained in Chapter 6.

Personal information

10.127 In IP 31, the ALRC asked whether the definition of personal information was adequate and appropriate in light of advances in technology.[165] The ALRC noted that, in some circumstances, information such as an individual's internet protocol (IP) address, mobile telephone number, email address or biometric information will not be personal information because it does not enable the identity of an individual 'reasonably [to] be ascertained from the information'.[166] In the context of RFID technology, it could be argued that information about tagged items in an individual's possession may not be personal information if the identity of the individual cannot 'reasonably be ascertained'. These types of information, however, may enable individuals to be monitored or profiled.

10.128 In Chapter 6, the ALRC recommends that 'personal information' be defined in the *Privacy Act* as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.[167] The recommended amendment to the definition of 'personal information' means that once information can be linked to an individual—and that individual is able to be monitored or targeted—it would become personal information for the purposes of the *Privacy Act*. The recommended definition would mean that forms of electronic communication such as telephone numbers, email addresses or IP addresses will become personal information for the purposes of the *Privacy Act*, once a sufficient amount of other information accretes around such points of contact.

Sensitive information

10.129 In IP 31, the ALRC asked whether the definition of sensitive information should include types of personal information collected by new technologies.[168] There was substantial support in submissions for amending the definition of 'sensitive information' to include biometric information. In Chapter 6, the ALRC recommends

---

164 Rec 51–1.
165 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 3–4.
166 In terms of the definition of 'personal information' in *Privacy Act 1988* (Cth) s 6(1).
167 Rec 6–1.
168 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.124].

that the definition of 'sensitive information' in the *Privacy Act* should be amended to include biometric information collected for the purpose of automated biometric verification or identification, and biometric template information.[169]

10.130 Biometric information shares characteristics with other types of sensitive information and should be subject to more stringent protection than non-sensitive personal information. Biometric information can be very difficult to replace once it has been accessed improperly. Further, biometric information may reveal other sensitive information about an individual, such as health, genetic, racial or ethnic information. The ALRC notes, however, that it is neither necessary nor practicable to classify all types of biometric information as 'sensitive information'. The recommended definition is intended to address the most serious privacy concerns around the handling of biometric information.[170]

Record

10.131 In Chapter 6, the ALRC recommends that the definition of 'record' in the *Privacy Act* should be amended to include a document (as defined in the *Acts Interpretation Act 1901* (Cth)) and information stored in electronic or other format. The *Acts Interpretation Act* defines a document to include an image, which covers photographs and other pictorial representations.[171]

169 Rec 6–4

170 The inclusion of certain types of biometric information in the definition of 'sensitive information' is discussed in Ch 6.

171 Rec 6–6.

11. Individuals, the Internet and Generally Available Publications

Contents

Introduction

11.1 The *Privacy Act 1988* (Cth) does not regulate the handling of personal information by individuals for the purposes of, or in connection with, their personal, family or household affairs.[1] This means that an individual acting in a personal capacity—for example, an individual who posts personal information about others on a personal 'blog'—is not regulated by the *Privacy Act.* In addition, while the privacy principles apply when personal information is collected by an agency or organisation for inclusion in a generally available publication, they do not apply to personal information that is held in a generally available publication. This is because the *Privacy Act* only applies to information held in a record, and a generally available publication (such as a publicly available website) is not a 'record' for the purposes of the *Privacy Act.*[2]

11.2 In this chapter, the ALRC first discusses whether the *Privacy Act* should regulate individuals acting in a personal capacity. It focuses on the regulation of one particular activity engaged in by individuals—namely, the publishing of personal

1 *Privacy Act 1988* (Cth) ss 7B(1), 16E.
2 Ibid s 6(1).

information in the online environment. The ALRC then discusses whether the *Privacy Act* needs to be amended to address issues about the online publication of publicly available information.

Individuals acting in a personal capacity

11.3 The development of new technologies has increased the ability of individuals to impinge on the privacy rights of others. For example, individuals can monitor the online activities of others through the use of spyware,[3] or disclose the email addresses of others in emails sent to numerous recipients.[4]

11.4 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* should be amended to cover any acts or practices of individuals relating to their personal, family or household affairs. The majority of stakeholders who answered this question opposed any such expansion of the scope of the Act.[5] For example, Electronic Frontiers Australia submitted that the *Privacy Act* is not 'an appropriate vehicle for application to the acts or practices of individuals relating to their personal, family or household affairs'. This was because it would be 'impractical and undesirable' to require individuals acting in a private capacity to comply with the requirements in the privacy principles.[6] Electronic Frontiers Australia submitted further that:

> the primary issues of concern are publication and/or public distribution and that collection and private use of information is generally of significantly less concern except under some particular circumstances.[7]

11.5 Similarly, the Office of the Privacy Commissioner (OPC) submitted that:

> the Privacy Act has been specifically tailored to regulate agencies and organisations and as such is ill-suited to the regulation of individuals in their personal capacity. For instance, it would be difficult and undesirable to require individuals to give notice or seek consent for collection of personal information. Also, applying data quality and data security principles to an individual's address book could be inappropriate.[8]

11.6 In Discussion Paper 72, *Review of Australian Privacy Law* (DP 72), the ALRC did not propose the expansion of the scope of the *Privacy Act* to regulate individuals acting in a non-commercial capacity. It noted, however, that the proposed statutory

---

3 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 244.

4 J Partridge, *Submission PR 26*, 4 June 2006.

5 See, eg, Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

6 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

7 Ibid.

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

cause of action for a serious invasion of privacy may be used against an individual acting in a non-commercial capacity as well as against an agency or organisation.[9]

Individuals and the internet

11.7 A major concern about individuals handling personal information relates to the content of information published by individuals on the internet. Individuals regularly use social networking and user-generated sites such as Facebook and YouTube to post photographs, videos and commentary that may interfere with the privacy of other individuals.[10] This phenomenon is often referred to as 'Web 2.0'.[11] Further, it has been estimated that there are at least 100 websites that contain images of people caught showering or undressing.[12]

11.8 Throughout the Inquiry a number of stakeholders expressed concern about the permanence of personal information published on the internet by individuals.[13] One stakeholder submitted that extensive personal information about herself and several family members was published on an amateur genealogy website in late 2006. The information was posted without the knowledge or consent of the individuals to whom it related. She noted that she had requested both the individual who owned the website and the relevant internet service provider (ISP) to remove the information, but that there was 'no one with the authority … to discover the source of this information or to have the information removed from the website'.[14] The Health Informatics Society of Australia informed the ALRC that individuals using online medical support forums sometimes publish personal information, including health information, about their relatives.[15]

---

9 In Ch 74, the ALRC recommends that the *Privacy Act* be amended to include a statutory cause of action for a serious invasion of privacy: Rec 74–1.

10 See, eg, P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

11 The term 'Web 2.0' can be used in various contexts. In this Report, it is used to refer to the social phenomenon where internet users—often individuals acting in a personal capacity—upload and distribute content such as text, photographs and videos.

12 C Calvert, *Voyeur Nation: Media, Privacy, and Peering in Modern Culture* (2000), cited in D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 100.

13 See, eg, Health Informatics Society of Australia, *Submission PR 554*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australia's National Computer Emergency Response Team, *Submission PR 474*, 14 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007; J Watts, *Submission PR 302*, 10 July 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

14 J Watts, *Submission PR 302*, 10 July 2007.

15 Health Informatics Society of Australia, *Submission PR 554*, 2 January 2008.

11.9 Currently, a procedure exists for removing offensive or illegal content that is accessible via the internet.[16] There is no similar procedure, however, for removing other privacy-invasive information published on the internet by an individual acting in his or her non-business capacity.

Take-down notices for online content?

11.10 In DP 72, the ALRC discussed the existing scheme for removing offensive or illegal content that is accessible via the internet.[17] The online regulation scheme, which is set out in sch 7 of the *Broadcasting Services Act 1992* (Cth), is administered by the Australian Communications and Media Authority (ACMA). In summary, ACMA can investigate complaints about content available via the internet. ACMA relies on the classification decisions of the Classification Board to determine whether content is 'prohibited content'.[18] If content is prohibited content, ACMA must direct the relevant internet content host to remove it. While it is not an offence to host prohibited content, if ACMA issues a take-down notice to an internet content host, the prohibited content must be removed as soon as practicable or, at the latest, by 6 pm the next business day. ACMA may issue an interim take-down notice while awaiting the outcome of classification of content by the Classification Board.[19]

11.11 Currently, the take-down scheme administered by ACMA cannot be used to make a complaint about, or seek the removal of, information posted on the internet which constitutes an invasion of an individual's privacy. The existing scheme's dependence on the *National Classification Code* and decisions of the Classification Board limits the extent to which the take-down notice procedure can be used. It is essentially an extension of the censorship scheme into the online environment and balances a number of competing interests.

> In relation to freedom of expression, [Schedule 7] is premised on the principle that what is illegal offline should also be illegal online. It does not provide for more onerous restrictions than those that apply to conventional media regulated under the Act. Definitions of prohibited material are based on specific and detailed criteria of the widely accepted national classification scheme administered by the Office of Film and Literature Classification. This scheme is designed to balance the public interest in allowing adults to read, hear and see material of their own choosing, with the public interest in protecting minors from material likely to harm or disturb them, and in protecting the community generally from offensive material.[20]

---

16 The Australian Communications and Media Authority (ACMA) can investigate complaints about content available via the internet. If satisfied that content is hosted in Australia and is 'prohibited content'—namely, content that has been given a certain classification by the Classification Board—or potentially prohibited content, ACMA must direct the relevant internet content host to remove the content: see *Broadcasting Services Act 1992* (Cth) sch 7.

17 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [8.10]–[8.16].

18 Prohibited content is content that is, or would be, classified as RC or X18+, or is classified R18+ and not subject to a restricted access system that complies with the criteria determined by ACMA: *Broadcasting Services Act 1992* (Cth) sch 7, cl 20.

19 Ibid sch 7, cl 47.

20 Australian Government Department of Communications, Information Technology and the Arts, *Review of the Operation of Schedule 5 to the Broadcasting Services Act 1992: Report* (2004), 14. The online regulation scheme was previously set out in sch 5 of the *Broadcasting Services Act 1992* (Cth).

11.12 As with any scheme regulating online content, the online content classification scheme has jurisdictional limitations. If the internet content is hosted outside Australia, ACMA is unable to issue a take-down notice. If prohibited content is sufficiently serious, however, ACMA can refer it to law enforcement authorities. ACMA can also request that ISPs take appropriate technical steps to minimise access to the material by end users in Australia.[21]

11.13 In DP 72, the ALRC asked whether the existing 'take-down' notice scheme that deals with internet content should be broadened to address privacy issues arising from the online publication of personal information.[22] The ALRC also asked, if a take-down notice scheme were to be implemented, what criteria should be used to assess whether an interference with privacy had taken place.[23]

Submissions and consultations

11.14 Some stakeholders supported the expansion of the existing take-down notice scheme to regulate the online publication of personal information. A number of youth organisations submitted that such a scheme would provide a useful avenue for the protection of the privacy of children and young people in the online environment.[24] For example, Youthlaw submitted that it has received a number of complaints from young people about the posting of photographs of them on the internet without their consent.[25] The Public Interest Advocacy Centre (PIAC) noted that, while in some circumstances the proposed statutory cause of action would provide a remedy for interferences with privacy on the internet, a separate take-down notice scheme

> would offer an effective alternative remedy to people who might not be able to afford legal representation, or who want to have the material removed from the internet immediately.[26]

11.15 Australia's National Computer Emergency Response Team (AusCERT) submitted that it currently seeks the removal of websites that could be used to facilitate the theft of personal information. In carrying out this work, it is reliant on the cooperation of parties such as ISPs or domain name registrars. AusCERT submitted that legislation making it an offence for a website to host such content could help to prevent the theft of personal information.[27]

11.16 Several stakeholders were not in favour of expanding the existing take-down notice scheme to deal with interferences with an individual's privacy. The Australian

---

21 *Broadcasting Services Act 1992* (Cth) sch 7, cls 62, 69.

22 The online regulation scheme is set out in Ibid sch 7.

23 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 8–1.

24 National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Youthlaw, *Submission PR 390*, 6 December 2007; Youth Affairs Council of Victoria Inc, *Submission PR 388*, 6 December 2007.

25 Youthlaw, *Submission PR 390*, 6 December 2007. The privacy of children and young people is discussed further in Chs 67, 68, 69.

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

27 Australia's National Computer Emergency Response Team, *Submission PR 474*, 14 December 2007. Identity theft is discussed further in Ch 12.

Government Attorney-General's Department stated that '[t]he regulation of online content is a complex one and such questions cannot be addressed in isolation'.[28] Another stakeholder submitted that such a scheme could have a negative impact on freedom of expression. This was because the potential costs of defending a legal action would be an incentive for an internet content host to remove content upon receipt of a take-down notice 'without due consideration or consultation'.[29] In addition, Telstra queried the effectiveness of an Australian-based scheme, noting that internet content can easily be moved to content hosts that are based overseas.[30]

11.17 A number of stakeholders addressed the criteria that should be used to determine when a take-down notice should be issued.[31] The National Children's and Youth Law Centre suggested that relevant criteria could include whether: an individual had consented to, or had a reasonable expectation of, online publication; an individual had suffered harm; and the publisher intended to abuse, harm or humiliate the individual to whom the information related.[32] The Special Broadcasting Service (SBS), however, submitted that

> it would be difficult to establish the objective criteria that would be necessary to make this proposal workable. Unlike the classification take-down regime which can refer to a set of ascertainable and easy to apply guidelines, any assessment as to whether material on the internet constituted an invasion of personal privacy would involve a complex case-by-case analysis. This would defeat the purpose of the proposal, that is, to provide an effective remedy for the unauthorised online publication of personal information.[33]

11.18 Other stakeholders queried which body would administer the suggested take-down notice scheme. ACMA noted that it did not have expertise in the adjudication of breaches of privacy, stating that its 'competence in regulating content arises from its remit of assessing material in accordance with Australia's classification scheme'.[34] In addition, the OPC did not believe it was 'best placed to issue take-down notices or deal with a complaint about such matters'. The OPC did not have a view on which body should administer a take-down notice scheme.[35]

11.19 Further, the OPC submitted:

> Given the broad variation in and use of online content, the Office considers that a separate, widespread, public consultation of community standards and views should be undertaken in any discussion related to take down notices and content that may constitute an invasion of an individual's privacy … Such public consultation could

---

28 Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.
29 S Hawkins, *Submission PR 382*, 6 December 2007.
30 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
31 See, eg, Special Broadcasting Service, *Submission PR 530*, 21 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.
32 National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007.
33 Special Broadcasting Service, *Submission PR 530*, 21 December 2007.
34 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007.
35 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

> also canvass community opinion on what criteria should be used to determine when a take down notice should be issued.[36]

11.20 Google Australia suggested that a privacy take-down notice scheme could be modelled on the safe harbour scheme for carriage service providers that is contained in the *Copyright Act 1968* (Cth).[37] In this scheme, an individual can issue a take-down notice to a carriage service provider if his or her copyright is infringed. If a carriage service provider complies with such a notice, it will not be liable for damages or any other civil remedy for copyright infringement.[38]

ALRC's view

11.21 It is not practical or desirable to expand the scope of the *Privacy Act* to regulate individuals acting in a non-commercial capacity. There are other methods that could deal more appropriately with situations where an individual acting in a personal capacity interferes with another individual's privacy. In Chapter 74, the ALRC recommends that the *Privacy Act* be amended to include a statutory cause of action for serious invasion of privacy.[39] As discussed in that chapter, the recommended statutory cause of action may be used against an individual acting in a non-commercial capacity, as well as against an agency or organisation.

11.22 The ALRC notes that much of the concern about individuals acting in a non-commercial capacity relates to information posted by individuals on websites. While a take-down notice scheme might help to address the circumstances where individuals refuse to remove from their website personal information about another person, the ALRC does not recommend the introduction of such a scheme.

11.23 A take-down notice scheme would require a decision maker to balance the right of freedom of expression and the right to individual privacy. In the ALRC's view, it is more appropriate for a court, rather than a regulator, to undertake such a balancing act. Finally, the ALRC queries the utility of an Australian take-down notice scheme, given the ease of moving internet content to a website hosted in another jurisdiction. The statutory cause of action for a serious invasion of privacy, therefore, is a more appropriate remedy.

---

36 Ibid.
37 Google Australia, *Submission PR 539*, 21 December 2007.
38 *Copyright Act 1968* (Cth) pt V div 2AA; *Copyright Regulations 1969* (Cth) pt 3A.
39 Rec 74–1.

11.24 The ALRC is mindful that the implementation of the statutory cause of action for a serious invasion of privacy, recommended in this Inquiry, will not address entirely the inherent difficulties in regulating the use and disclosure of personal information published on the internet.[40] For example, while the *Privacy Act* has extraterritorial application, enforcing an order made by an Australian court in an action for serious invasion of privacy against a website hosted overseas may be difficult.[41] In addition, information posted online can be copied onto an infinite number of other websites within seconds. It may be time consuming and costly—if not impossible—to remove altogether privacy invasive information from the internet.[42]

11.25 Accordingly, it is necessary to educate individuals about the impact on their privacy and that of others that may result from posting personal information online. While online education programs should not be directed only towards children and young people, the ALRC notes the importance of early education on the impact of the internet on privacy. In Chapter 67, the ALRC recommends that, to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, and in particular privacy in the online environment, into school curriculums.[43] Further, the OPC, in consultations with ACMA, should ensure that specific guidance on the privacy aspects of using social networking sites is developed and incorporated into publicly available educational material.[44]

Generally available publications

11.26 Personal information about a substantial number of people is available from public sources such as electoral rolls, court records, state registers of births, deaths and marriages, annual reports and newspapers. This information may be of interest to people for a multitude of reasons. For example, it may be of interest to: people engaged in direct marketing or fundraising; employers wishing to investigate potential employees; politicians wishing to know more about their constituents or vice versa; people wishing to use false identities to engage in illegal activities; and law enforcement officers investigating criminal offences.

11.27 In the past, individuals seeking to obtain access to generally available publications usually were required to attend the location where the information was stored, such as a court house, and to expend a considerable amount of time manually searching or copying records.[45] This meant that personal information in generally available publications was afforded a degree of de facto privacy protection.

---

40 Remedies for a successful action for invasion of privacy are discussed in Ch 74.

41 *Privacy Act 1988* (Cth) s 5B.

42 For a discussion of the recent failure of a judicial order to remove from the internet the content contained on a particular website, see D Gillmor, 'Freedom of Information', *The Guardian* (online), 25 February 2008, <commentisfree.guardian.co.uk>.

43 Rec 67–3.

44 Rec 67–2.

45 D Solove, 'Access and Aggregation: Privacy, Public Records and the Constitution' (2002) 86 *Minnesota Law Review* 1137, 1152.

Developments in information and communications technologies, such as the creation of powerful computer databases and the internet, have greatly altered the way in which information is stored, accessed, combined, transferred and searched.[46] In particular, information can now be published in electronic form. While it is arguable that information in the public domain should be available in all formats, it also can be argued that privacy 'can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible'.[47]

11.28 The publication of publicly available information in electronic form increases the ability of third parties to combine disparate pieces of personal information about others.[48] Disparate pieces of information about a person may reveal little when viewed separately, but the aggregation of these pieces of information—for example, in the search results provided by an internet search engine in response to a search query about a person's name—can provide a detailed profile of a person. Internet search engines and social networking sites can be used by third parties to obtain information about individuals for a number of purposes. For example, a recent United Kingdom study noted that one in five employers searched the internet for information about job applicants.[49] In addition, personal information about an individual published on the internet can be used to conduct identity theft.[50] Another issue is that information aggregated from a variety of different publicly available sources may present an inaccurate portrait of an individual if, for example, inaccurate information were collected, or errors occurred, during the aggregation process.

Application of the *Privacy Act*

11.29 The privacy principles apply when personal information is collected by an agency or organisation for inclusion in a 'record' or a 'generally available publication'.[51] The privacy principles that deal with the handling of personal information subsequent to collection, however, only apply to personal information that is held in a record.[52] A record is a document, database, or photograph or other pictorial representation of a person.[53] A book, magazine or other publication that is generally available to the public is not a record for the purposes of the *Privacy Act*.[54]

---

46 Ibid, 1152–1153.

47 Ibid, 1178.

48 M Neave, 'International Regulation of the Publication of Publicly Accessible Personal Information' (2003) 10 *Privacy Law & Policy Reporter* 120, 122.

49 YouGov, *What Does Your NetRep Say About You? [Research Commissioned by Viadeo]* (2007).

50 Identity theft is discussed in Ch 12.

51 *Privacy Act 1988* (Cth) s 14, IPPs 1–3 and s 16B(1).

52 Ibid s 14, IPPs 4–11 and s 16B(2).

53 Ibid s 6(1). In Ch 6, the ALRC recommends that the definition of 'record' should be amended to make it clear that a record includes a document as defined in the *Acts Interpretation Act 1901* (Cth), and information stored in electronic or other format: Rec 6–6.

54 Ibid s 6(1). In Ch 6, the ALRC recommends that the definition of a generally available publication should be amended to clarify that a publication is generally available whether or not a fee is charged for access to the publication: Rec 6–7.

11.30 The Supreme Court of Victoria has considered the public nature of websites in the context of deciding whether confidential information loses its confidential nature when published online by anonymous bloggers.[55] In the privacy context, the relevant consideration for determining whether a publication is generally available is whether access to that publication can be obtained by the public. Guidance issued by the OPC indicates that websites that are not encrypted or password protected are considered 'generally available'.[56]

11.31 There are, however, some restrictions on the handling of personal information contained in a generally available publication. An agency or organisation that continues to hold personal information that has been made generally available in a record—for example, a master copy—will need to comply with the requirements in the privacy principles for the protection of personal information that is held in the record.[57] Moreover, an agency or organisation that collects personal information from a generally available publication for inclusion in a record or another generally available publication will need to comply with the requirements in the relevant privacy principles.[58] For example, the 'Collection' principle requires an agency or organisation to collect personal information about an individual only from that individual if it is reasonable and practicable to do so. In addition, the 'Notification' principle requires an agency or organisation that collects personal information about an individual other than from the individual concerned to take such steps, if any, as are reasonable in the circumstances to notify or ensure that the individual is aware of the requirements of the principle.[59]

11.32 This section provides an overview of two sources of publicly available information—public registers and court records.

Public registers

11.33 In the late 19th century, governments began systematically to compile and retain records of their citizens. Today, records are kept 'for almost every occasion an individual comes into contact with the state bureaucracy'.[60] Legislation may require these records to be used to create public registers. For example, the *Commonwealth Electoral Act 1918* (Cth) requires the Australian Electoral Commission to construct

---

55 In deciding that confidential information does not lose its confidential nature by such publication, Kellam J stated that an unknown number of internet users had viewed the website in question. Further, the public does not have the 'expectation of authenticity, veracity or otherwise of the information posted on such websites': *Australian Football League v The Age Company Ltd* [2006] 15 VR 419, 431.

56 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003); Office of the Federal Privacy Commissioner, *Guidelines for Federal and ACT Government Websites* (2003) <www.privacy.gov.au/internet/web/> at 1 May 2008.

57 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003), 3.

58 See the 'Collection', 'Notification' and 'Data Quality' principles, which are set out at the beginning of this Report.

59 The 'Notification' principle applies in circumstances where a reasonable person would expect to be notified.

60 D Solove, 'Access and Aggregation: Privacy, Public Records and the Constitution' (2002) 86 *Minnesota Law Review* 1137, 1143.

and maintain a roll of people eligible to vote at federal, and, by agreement, most state and local government elections. Electoral rolls are available for public inspection without fee at offices of the Australian Electoral Commission.[61]

11.34 Public registers often promote important public interests. For example, a publicly available electoral roll facilitates the conduct of free and fair elections by 'enabling participants to verify the openness and accountability of the electoral process and object to the enrolment of any elector'.[62] There is, however, a tension between the public interests served by a public register of information and the privacy of individuals included on the register. This is exacerbated when it is compulsory to provide the information that is included in the register.[63]

11.35 It has been argued that failure to adequately protect the privacy of personal information contained in public registers can have serious consequences. For example, individuals may choose to withdraw from public life in order to protect their privacy.[64] Concern has been expressed that the widespread dissemination of electors' personal information 'has the potential to discourage some electors from enrolling and exercising their democratic rights and duties'.[65] Research conducted for the OPC indicated that only 19% of survey participants believed that businesses should be allowed to use the electoral roll for marketing purposes.[66]

11.36 Legislation establishing a public register also can limit the use and disclosure of information acquired from the register. For example, s 177 of the *Corporations Act 2001* (Cth) prohibits any person from using information collected from a shareholder register to contact a shareholder.[67] Legislation can limit the use and disclosure of information acquired from a register that is published in electronic form. For example, the *Commonwealth Electoral Act 1918* (Cth) prohibits a person from using electoral roll information provided by the AEC in tape or disk format, unless the disclosure is in connection with an election or referendum, or monitoring the accuracy of information contained in a roll or other prescribed purpose.[68]

---

61 *Commonwealth Electoral Act 1918* (Cth) s 90A.

62 Australian Electoral Commission, *How to View the Commonwealth Electoral Roll* <www.aec.gov.au/Enrolling_to_vote/About_Electoral_Roll/How_to_view_electoral_roll.htm> at 1 May 2008.

63 For example, it is compulsory for individuals who are entitled to have their names included on an electoral roll to enrol within 21 days of becoming so entitled: *Commonwealth Electoral Act 1918* (Cth) s 101.

64 See B Givens, *Public Records on the Internet: The Privacy Dilemma* (2002) Privacy Rights Clearinghouse <www.privacyrights.org/ar/onlinepubrecs.htm> at 1 May 2008.

65 Australian Electoral Commission, *Submission to the Joint Standing Committee on Electoral Matters Inquiry into the 2001 Federal Election*, 1 July 2002, App D, 8.

66 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), [6.4].

67 Ch 16 discusses collection of personal information that is required or authorised by law.

68 *Commonwealth Electoral Act 1918* (Cth) s 91A(2A). This provision does not apply to a Senator, member of the House of Representatives, or political party.

11.37 In February 2008, the New Zealand Law Commission (NZLC) released a report on the law relating to public registers.[69] This report considered whether the law relating to public registers required systematic alteration as a result of privacy considerations and emerging technology. The NZLC expressed the view that any regulatory model for public registers should:

- be compatible with the principles of openness and transparency;
- ensure that agencies administering public registers are accountable for the fair handling of personal information;
- allow an appropriate decision maker, usually Parliament, to balance various public interests when determining whether personal information should be accessible on a public register;
- be flexible enough to address the diversity of public registers and be able to accommodate changes in policy and technology; and
- be administratively simple, efficient and cost-effective, and capable of operating effectively in the online environment.[70]

11.38 The NZLC discussed four possible regulatory models: (1) maintaining the current system of regulation of some registers by the *Privacy Act 1993* (NZ), making amendments where appropriate; (2) creating a rebuttable system of general access to public registers; (3) creating a public register statute that sets out principles and provisions applicable to all public registers; and (4) regulating public registers through their individual establishing statutes. The NZLC concluded that the fourth option was preferable. It recommended a review of all public registers according to a template of considerations, with any changes to be introduced in an omnibus Bill.[71] This mechanism would have the advantage of legislative clarity and certainty. Further, it would require Parliament to balance relevant public and private interests at the stage of setting up or amending each register.

Court records

11.39 The principle of open justice is an essential feature of the common law judicial tradition. It requires the administration of justice to be conducted in open court. The principle of open justice 'is an important safeguard against judicial bias, unfairness and incompetence, ensuring that judges are accountable in the performance of their duties'.[72] In 2006, the NZLC noted that the principle of open justice generally requires open access to court records.[73]

---

69 New Zealand Law Commission, *Public Registers—Review of the Law of Privacy, Stage 2*, Report 101 (2008).
70 Ibid, 71.
71 Ibid, 71–75.
72 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), [2.2].
73 Ibid, [2.4].

11.40 Court records often contain vast amounts of personal information about a number of people, including the parties, family members of the parties and witnesses. For example, records of bankruptcy cases may include details of the financial circumstances of bankrupts; records of cases in which damages are claimed may include detailed information regarding the health of the plaintiff; records of family court proceedings may contain detailed information about family relationships; and records of criminal cases may include information about an offender's previous criminal history, social security status or mental health.

11.41 Access to court records is regulated by legislation and rules of court.[74] In the Federal Court of Australia, a person is entitled to search and inspect certain documents, such as pleadings, judgments or orders, unless the court or a judicial officer has ordered that they are confidential.[75] A person who is not a party to the proceeding may only inspect certain documents, such as interrogatories or answers to interrogatories, with the leave of the court.[76] Leave usually will be granted, however, where a document has been admitted into evidence or read out in open court.[77]

11.42 Section 121 of the *Family Law Act 1975* restricts the publication of court proceedings that would identify a party, witness or person related to proceedings. 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 of Australia has adopted a policy and practice for the making of personal information contained in court judgments made available for publication anonymous or pseudonymous. In addition, the Supreme Court of New South Wales recently has introduced an identity theft prevention and anonymisation policy for transcripts and judgments. The policy requires judges to consider whether it would be appropriate to restrict the publication of details such as the dates of birth and residential addresses of victims, witnesses and accused.[78]

Options for reform

11.43 There are various approaches to regulate online access to personal information contained in generally available publications. Overseas jurisdictions differ in the way in which they approach the issue. For example, some Scandinavian countries allow a substantial amount of personal information to be included in government records

---

74 See, eg, *High Court Rules 2004* (Cth) r 4.07.4; *Federal Court Rules 1979* (Cth) o 46 r 6; *Federal Magistrates Court Rules 2001* (Cth) r 2.08. In Ch 35, the ALRC discusses the partial exemption of federal courts from the operation of the *Privacy Act 1988* (Cth). The ALRC also recommends that 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: Rec 35–1.

75 *Federal Court Rules 1979* (Cth) o 46 r 6(1), (2).

76 Ibid o 46 r 6(3), (5).

77 Federal Court of Australia, *Public Access to Court Documents* <www.fedcourt.gov.au/courtdocuments/publicdocuments.html> at 1 May 2008.

78 Supreme Court of New South Wales, *Identity Theft Prevention and Anonymisation Policy* (2007).

published on public websites.[79] At the other end of the spectrum, a Bill currently under consideration in New Zealand is intended to prevent access to births, deaths and marriages publications that were produced less than 100 years ago.[80]

11.44 In DP 72, the ALRC noted that there were several ways to restrict inappropriate internet publication of personal information, including to:

- prohibit the collection of personal information contained in generally available publications;
- restrict the use and disclosure of publicly available information in electronic form to that which is consistent with the public interest served by publishing the information;
- limit the type of information that is made available electronically to that which is necessary to promote the purpose of the public record; and
- remove unnecessary personal information from documents before they are published electronically.[81]

11.45 In DP 72, the ALRC noted that in the online environment it could be difficult to enforce the first two options for reform. The ALRC suggested that a better approach would be for the OPC to provide education and guidance to agencies and organisations directed towards restricting the type and extent of personal information that is made available online.[82] The ALRC noted that the Office of the Victorian Privacy Commissioner (OVPC) has issued guidelines to Victorian state agencies that collect personal information for inclusion on public registers. These guidelines outline circumstances where it is appropriate for an agency to give notice about online dissemination of personal information and where the online dissemination of information should be suppressed.[83]

11.46 The ALRC proposed that OPC guidance should: apply whether or not the agency or organisation is required by law to make the personal information publicly available; set out certain factors that agencies and organisations should consider before publishing personal information in an electronic form; and set out the requirements in the model Unified Privacy Principles (UPPs) with which agencies and organisations

---

79 For a discussion of the significant number of Swedish government records that are published online, see E Addley, 'Sweden Tries to Lose Reputation as Snoopers' Paradise', *Guardian Unlimited Technology* (online), 19 June 2007, <technology.guardian.co.uk>.

80 See, eg, Births, Deaths, Marriages, and Relationships Registration Amendment Bill 2007 (NZ).

81 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [8.53]–[8.55].

82 Ibid, Proposal 8–1.

83 Office of the Victorian Privacy Commissioner, *Public Registers and Privacy—Guidance for the Victorian Public Sector* (2004).

need to comply when collecting personal information from generally available publications.[84]

Submissions and consultations

11.47 A number of stakeholders supported this proposal.[85] The OVPC suggested that, to ensure efficiency and consistency, the proposed guidance should be produced jointly by privacy commissioners in all Australian jurisdictions and should apply to agencies, organisations and state and territory agencies.[86]

11.48 The Cyberspace Law and Policy Centre submitted that the OPC guidance should encourage a presumption that personal information should not be posted online 'unless all alternatives have been explored and rejected as not feasible, or the competing social interests clearly justify such a level of Internet publication'. Further, agencies or organisations should be encouraged to notify individuals before online publication of their personal information, and provide a way for individuals to challenge the decision to publish the information online.[87]

Public registers

11.49 In PIAC's view, guidance would not restrict the electronic publication of personal information contained on public registers. PIAC suggested that stronger regulation was required to prevent the profiling of an individual from information collected from generally available publications.[88]

11.50 PIAC submitted that legislation establishing public registers should be reviewed to ensure that there are appropriate restrictions on the type and extent of personal information published on the internet, and that any restrictions on the use and disclosure of personal information contained on the register are clearly set out. PIAC submitted that these legislative instruments should limit publicly available information that is published in an electronic form to that which is necessary to promote the purpose of the public record, or provide for the removal of unnecessary personal information from documents before they are published electronically.[89]

---

84 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 8–1.

85 See, eg, Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

86 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. In Ch 17, the ALRC recommends that, when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies that handle personal information, the Australian Government agency should ensure that a memorandum of understanding or other arrangement is in place to ensure appropriate handling of personal information: Rec 17–1.

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

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

89 Ibid.

Court records

11.51 A number of courts and tribunals have advised the ALRC that they have developed internal policies and guidelines that relate to the online publication of judgments. This guidance is developed by each court and tribunal and is directed towards the particular issues that arise from the online publication of judgments in each jurisdiction. For example, a court that deals mainly with family law matters may require different procedures about the redaction of personal information in judgments published online than a court that deals mainly with commercial matters.

11.52 The OPC noted that the publication of court records could interfere with spent convictions laws, facilitate identity theft and lead to intimidation of those involved in court processes. The OPC was of the view, however, that 'changes to court record publication are best dealt with through procedural directives or guidelines rather than through legislative intervention'.[90] The OPC submitted that a coordinated approach between state, territory and federal courts 'would provide a more consistent framework for the electronic publication of court records'. The OPC suggested that it would be appropriate for the Standing Committee of Attorneys-General (SCAG) to consider this issue.[91] The Cyberspace Law and Policy Centre supported a separate inquiry into the publication of electronic court records.[92]

ALRC's view

11.53 The internet has changed the nature of the 'public domain'. It is not appropriate to deal with the issues presented by the electronic publication of publicly available information by increasing the regulation of personal information held in a 'generally available publication'. There is a public interest in making certain types of information publicly available. In some circumstances, this public interest remains relevant for generally available publications published in an electronic form. In addition, it is difficult to enforce the collection, use and disclosure of personal information in such publications. Electronic publication of generally available publications has increased, rather than decreased, the difficulties of enforcement.

11.54 The ALRC observes that stakeholders' concerns about generally available publications are focused on circumstances when these publications are widely disseminated—in particular, when they are posted on the internet. As discussed above, there are inherent difficulties in regulating the collection, use and disclosure of personal information published on the internet. Agencies and organisations should, therefore, be encouraged to put restrictions on the type and extent of personal information that is published on the internet.

11.55 In the case of public registers, the electronic publication of the register may be regulated by the legislative instrument that establishes the register—in the way that, for

---

90 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
91 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
92 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

example, the *Commonwealth Electoral Act* regulates certain uses and disclosures of information collected from electronic versions of the electoral roll. In the ALRC's view, individual legislative instruments that establish public registers should be reviewed to ensure each instrument sets out clearly any restrictions on the electronic publication of personal information contained on a register. Such a review could be based on the template discussed by the NZLC in its report on regulatory models for public registers. This approach will ensure that an appropriate balancing between the public interests of openness and transparency and the privacy interests of individuals is undertaken for each register.

11.56 The ALRC notes that courts and tribunals that publish judgments and decisions in the online environment have developed internal policies and guidelines that deal with particular issues that arise in the relevant jurisdiction. In the ALRC's view, the content of court and tribunal records should remain within the purview of the court or tribunal in question. The ALRC also notes that SCAG is considering the issue of online publication of criminal records in relation to spent convictions.[93]

11.57 In addition, the OPC should provide education and further guidance to agencies and organisations addressing the restrictions that should be placed on the type and extent of personal information published online. The ALRC notes that the OPC has issued an Information Sheet (Information Sheet 17) that focuses on the collection by organisations of personal information contained in generally available publications.[94] Information Sheet 17 also lists some tips for good privacy practice that apply to agencies and organisations required by law to make personal information publicly available. In addition, the OPC recently conducted an own motion investigation into the publication of insolvency information on the website of a trustee firm. In its decision, the OPC recommended that the firm take steps to prevent general internet users from browsing the bankruptcy files. The OPC suggested that one way to ensure that creditors could obtain access to the information would be to secure it using password protection.[95]

11.58 Information Sheet 17 could be used as the basis for providing more detailed guidance to agencies and organisations that make personal information about individuals available in electronic form. The guidance should apply whether or not the agency or organisation is required by law to make the personal information publicly available. The guidance could provide detailed advice on issues outlined in Information Sheet 17—for example, factors that agencies and organisations should consider before publishing personal information in an electronic form, such as whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual. The guidance could also provide examples of when it might be appropriate to restrict access to information by way of

---

93 Standing Committee of Attorneys-General, 'Communiqué' (Press Release, 28 March 2008).

94 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003).

95 *Own Motion Investigation v Bankruptcy Trustee Firm* [2007] PrivCmrA 5. An exemption from the *Privacy Act* for insolvency practitioners is considered, but not recommended, in Ch 44.

password protection, and what type of information should be suppressed in a generally available publication that is published online.

11.59 The recommended guidance should also set out clearly the requirements with which both agencies and organisations must comply when collecting information from generally available publications for inclusion in a record (or another generally available publication). The ALRC notes that the definition of a 'record' includes a 'database'.[96] It is highly unlikely that personal information collected from generally available publications—for example, by an organisation for the purposes of direct marketing or data-matching—will not be included in some form of record (or another generally available publication).[97] The recommended guidance should set out the steps that should be taken by an agency or organisation that collects personal information from generally available publications to meet the obligations in the 'Collection', 'Notification', 'Data Quality' and 'Direct Marketing' principles.[98]

11.60 Finally, the ALRC notes that both the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) regulate personal information that is collected for inclusion in a record or generally available publication, but the principles only apply to personal information that is held in a record. The way that this is achieved in the legislation, however, differs. IPPs 1–3 refer to both a 'record' and a 'generally available publication', whereas IPPs 4–11 refer only to a 'record'. In relation to the NPPs, the application of the relevant principles to records and generally available publications is set out in s 16B. In the ALRC's view, the latter approach is preferable and notes that it will be necessary to make a consequential amendment to s 16B of the *Privacy Act* when the model UPPs are implemented.[99]

Recommendation 11–1 The Office of the Privacy Commissioner should develop and publish guidance that relates to generally available publications in an electronic format. This guidance should:

(a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;

(b) set out the factors that agencies and organisations should consider before publishing personal information in an electronic format (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and

96 *Privacy Act 1988* (Cth) s 6(1). The definition of a 'record' is discussed further in Ch 6.

97 In Ch 10, the ALRC proposes that the OPC develop and publish guidance on data-matching to organisations: Rec 10–4.

98 The 'Collection', 'Notification' and 'Data Quality' principles apply to both agencies and organisations. The 'Direct Marketing' principle only applies to organisations.

99 The model Unified Privacy Principles are discussed in Part D.

(c) clarify the application of the model Unified Privacy Principles to the collection of personal information from generally available publications for inclusion in a record or another generally available publication.

Recommendation 11–2 The Australian Government should ensure that federal legislative instruments establishing public registers containing personal information set out clearly any restrictions on the electronic publication of that information.

12. Identity Theft

Contents

Introduction

12.1 In this chapter, the ALRC discusses a potential consequence of an interference with the privacy of an individual—identity theft. The definition of identity theft, and existing responses to it in Australia and overseas, are discussed. In particular, recent moves to criminalise identity theft in Australia are considered. An overview of the ways in which privacy laws can assist in preventing identity theft, and minimising the harm caused by it after it has occurred, is then provided. Specific reforms of privacy laws that may help to address the problem of identity theft are discussed in further detail throughout this Report.

12.2 Identity theft has existed for centuries. It has been argued, however, that it is becoming more prevalent in today's society because of developments in technology.[1] For instance, developments in information and communications technology mean that agencies and organisations now store vast amounts of identifying information electronically. Any breach of the secure storage of this information can increase the risk of identity theft for the people to whom the stored identifying information relates.

1 See, eg, N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 1; R Lozusic, *Fraud and Identity Theft: Briefing Paper 8/2003* (2003) Parliament of New South Wales—Parliamentary Library.

Further, electronic commerce and electronic government create impersonal transacting environments that are conducive to identity crime, and developments in computer technology have greatly increased the ability of individuals to forge identifying documents.[2]

What is identity theft?

12.3 While there is widespread concern about identity theft and its impact on privacy, there is little consensus about the definition of the term 'identity theft'. Commentators, legislators and policy makers tend to use the terms 'identity crime', 'identity fraud' and 'identity theft' in differing ways and, at times, interchangeably.

12.4 In this Report, 'identity crime' is used broadly to describe any offence committed using a fabricated, manipulated or stolen identity.[3] 'Identity fraud' is used to describe a type of identity crime—namely, the gaining of a benefit (or the avoidance of an obligation) through the use of a fabricated, manipulated or stolen identity. 'Identity theft' 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.[4]

12.5 Identity theft can be committed for a number of reasons. For example, as noted above, the assumption of another person's identity can facilitate the commission of identity crimes, including identity fraud, people smuggling and terrorism offences.[5] It can also enable a person to avoid detection in order to avoid meeting obligations, such as making child support payments. Alternatively, identity theft may be committed simply to distress or intimidate the person to whom the illicitly acquired identity information relates.[6]

12.6 There are many ways in which identifying information about another person can be acquired surreptitiously, including through the theft of a person's mail, wallet, purse or handbag, or through the retrieval of documents from a person's rubbish. The identifying information of another person can also be acquired through more sophisticated means, such as skimming the person's credit card or hacking into an electronic database containing identifying information about the person.[7] Social engineering and 'phishing' are other methods used to acquire information in the online environment. Phishing typically occurs when an email purporting to be from a trusted

---

2 See, eg, S Cuganesan and D Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent* (2003) Securities Industry Research Centre of Asia-Pacific, 1.

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 Ibid, 15.

5 Australasian Centre for Policing Research, *Australasian Identity Crime Policing Strategy 2006–2008 of the Australasian and South West Pacific Region Police Commissioners' Conference* (2005), 1.

6 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Discussion Paper, Model Criminal Code Chapter 3, Credit Card Skimming Offences* (2004), 31.

7 N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 5–6.

entity directs a recipient to a website that closely resembles the website of that entity. The 'phisher' can then acquire any information the person enters on the 'fake' website, such as the person's name or online banking password.[8] Social engineering practices, such as pretexting, rely on a person providing information to another person, whether face-to-face or over the telephone or internet.[9] In addition, details posted by a person on a social networking site or online profile can be sufficient to enable the theft of that person's identity by another person accessing that profile.[10]

12.7 Identity theft can be a traumatic experience for the person whose identifying information is stolen. Victims of identity theft may suffer direct financial loss as a result of the theft. In addition, they may incur costs when attempting to prevent the continued use of their identifying information. Further, victims of identity theft are often required to expend large amounts of time and effort countering the adverse effects of the theft. For example, they may be required to restore their credit rating, or correct errors in their criminal history.[11]

How prevalent is it?

12.8 In August 2007, a *Community Attitudes to Privacy* survey was prepared for the Office of the Privacy Commissioner (OPC).[12] Sixty percent of respondents were concerned about becoming the victim of identity theft or fraud. Nine percent of respondents to the survey claimed to have been the victim of identity theft or fraud.[13] Apart from this, there is very little information about the prevalence of identity theft in Australia. This is partly because the acquisition of the information is not generally a criminal offence. Rather, it is the later use of the information for certain purposes that attracts criminal liability. This makes it difficult to locate information about rates of identity theft. In addition, not all instances of identity theft are reported to authorities or otherwise disclosed. Agencies and organisations in particular may be reluctant to report identity theft for fear that it will cause damage to their reputations or expose weaknesses in their security systems.[14]

---

8 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Discussion Paper—Identity Crime* (2007), 5.

9 United States Computer Emergency Readiness Team (US-CERT), *National Cyber Alert System—Avoiding Social Engineering and Phishing Attacks* (2004) <www.us-cert.gov/cas/tips/ST04-014.html> at 24 April 2008.

10 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Final Report—Identity Crime* (2008), 6.

11 See J Blindell, *Review of the Legal Status and Rights of Victims of Identity Theft in Australasia* (2006) Australasian Centre for Policing Research, 5.

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

13 Ibid, 67–68.

14 N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 3.

12.9 In 2000, the House of Representatives Standing Committee on Economics, Finance and Public Administration recommended that Australian governments and industries work together to develop national statistics on the extent and cost of identity fraud.[15] In response to this recommendation, the Australian Transaction Reports and Analysis Centre's Steering Committee on Proof of Identity commissioned a report on the nature, cost and extent of identity fraud in Australia. This report found that the cost of identity fraud to Australia in 2001–02 was approximately $1.1 billion.[16] This estimate included the costs associated with preventing, detecting and responding to identity fraud, as well as losses directly incurred as a result of the fraud.[17] Unfortunately, given its focus on identity fraud, which includes fraud committed using fictitious identity information, this report does little to illuminate the full extent or cost of identity theft in Australia.

12.10 In 2003, the Australian Institute of Criminology and PricewaterhouseCoopers released the results of a study of 155 serious fraud prosecutions completed in Australia and New Zealand in 1998 and 1999.[18] Stolen identities were used in approximately 13% of the cases studied.[19] In 2007, the United States Federal Trade Commission (FTC) released a report that contained the results of an identity theft survey. With reference to these results, the FTC suggested that approximately 8.3 million adults in the United States were the victims of identity theft in 2005.[20]

Criminalising identity theft

Federal legislation

12.11 Currently, identity theft is not a federal offence in Australia. There are, however, numerous federal offence provisions that can be used to prosecute offenders who use illicitly acquired personal information when engaging in certain activities. These include offence provisions in the *Criminal Code* (Cth),[21] as well as in other pieces of federal legislation, such as the *Financial Transaction Reports Act 1988* (Cth)[22] and the *Migration Act 1958* (Cth).[23]

---

15 Parliament of Australia—House of Representatives Standing Committee on Economics Finance and Public Administration, *Numbers on the Run—Review of the ANAO Report No 37 1998–99 on the Management of Tax File Numbers* (2000), rec 18.

16 S Cuganesan and D Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent* (2003) Securities Industry Research Centre of Asia-Pacific, 55.

17 Ibid, Ch 5.

18 Australian Institute of Criminology and PricewaterhouseCoopers, *Serious Fraud in Australia and New Zealand*, Australian Institute of Criminology Research and Public Policy Series No 48 (2003).

19 Ibid, 2.

20 United States Federal Trade Commission, *2006 Identity Theft Survey Report* (2007), 4.

21 See, eg, *Criminal Code* (Cth) ss 134.1 (obtaining property by deception), 134.2 (obtaining a financial advantage by deception), 135.1 (general dishonesty), 135.2 (obtaining financial advantage), 135.4 (conspiracy to defraud).

22 See, eg, *Financial Transaction Reports Act 1988* (Cth) s 24 (opening account, etc in false name).

23 See, eg, *Migration Act 1958* (Cth) s 234 (false papers etc).

12.12 In 2000, the House of Representatives Standing Committee on Legal and Constitutional Affairs concluded that the offences to be inserted into the *Criminal Code* (Cth) by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 1999* (Cth) dealt adequately with criminal conduct related to identity fraud.[24]

12.13 Nevertheless, in 2004 a new Part containing 'financial information offences' was inserted into Chapter 10 of the *Criminal Code*.[25] Accordingly, it is now a federal offence dishonestly to obtain or deal in personal financial information without the consent of the person to whom the information relates.[26] The definition of 'personal financial information' is broad and includes all information relating to a person that may be used, alone or in conjunction with other information, to access funds, credit or other financial benefits.[27]

12.14 The financial information offences in the *Criminal Code* were intended to address credit card skimming—the illicit capturing or copying of legitimate credit card data[28]—and internet banking fraud.[29] They appear, however, to be broad enough to cover many instances of identity theft.

12.15 In March 2008, the Model Criminal Code Law Officers Committee released a report on identity crime.[30] Using the term 'identity crime' to refer to practices including identity theft and identity fraud, the Committee recommended the creation of three identity crime model offences that relate to:

- dealing in identification information;
- possession of identification information with the intention of committing, or facilitating the commission of, an indictable offence; and
- possession of equipment to create identification information, in certain circumstances.[31]

---

24 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999* (2000), [3.8]–[3.10].

25 *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No 2) 2004* (Cth) sch 3.

26 *Criminal Code* (Cth) s 480.4.

27 Ibid s 480.1(1).

28 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Discussion Paper, Model Criminal Code Chapter 3, Credit Card Skimming Offences* (2004), 1. This Committee has recently been renamed the Model Criminal Law Officers Committee.

29 Commonwealth, *Parliamentary Debates*, House of Representatives, 4 August 2004, 32035 (P Slipper), 32036–32037.

30 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Final Report—Identity Crime* (2008).

31 Ibid, 25–41.

12.16 At the time of writing in April 2008, the Standing Committee of Attorneys-General had agreed to prepare a review paper examining the implementation priorities of the Committee's report.[32]

State and territory legislation

12.17 In the majority of Australian states and territories, it is not an offence to assume or adopt another person's identity. There are, however, numerous state and territory offences that can be used to prosecute offenders who use illicitly obtained identity information to commit criminal offences.[33]

12.18 In some circumstances, however, identity theft is a criminal offence in South Australia. Section 144B of the *Criminal Law Consolidation Act 1935* (SA) makes it an offence to assume the identity of another person (whether living or dead, real or fictional, natural or corporate) with the intent to commit, or facilitate the commission of, a 'serious criminal offence'.[34] Section 144C makes it an offence to use the 'personal identifying information' of a living or deceased person, or a body corporate, with the intent to commit, or facilitate the commission of, a serious criminal offence. In March 2007, similar offence provisions were enacted in Queensland.[35]

Other jurisdictions

12.19 In October 1998, the United States Congress passed the *Identity Theft and Assumption Deterrence Act of 1998* (US). This Act makes it a federal offence, punishable by up to 15 years imprisonment or a fine of US$250,000, to

> knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law'.[36]

12.20 The *Identity Theft Penalty Enhancement Act of 2004* (US) establishes penalties for the offence of aggravated identity theft.[37] Identity theft is also an offence in the vast majority of states in the United States.[38]

---

32 Standing Committee of Attorneys-General, 'Communiqué' (Press Release, 28 March 2008).

33 See R Smith, 'Examining the Legislative and Regulatory Controls on Identity Fraud in Australia' (Paper presented at Marcus Evans Conferences, Corporate Fraud Strategy: Assessing the Emergency of Identity Fraud, Sydney, 25–26 July 2002).

34 A 'serious criminal offence' is an indictable offence or an offence prescribed by regulation: see *Criminal Law Consolidation Act 1935* (SA) s 144A.

35 The *Criminal Code and Civil Liability Amendment Act 2007* (Qld) s 6 inserts a new section into the *Criminal Code Act 1899* (Qld), which in certain circumstances makes it an offence to obtain or deal with identification information: *Criminal Code Act 1899* (Qld) s 408D.

36 *Identity Theft and Assumption Deterrence Act of 1998* 18 USC § 1028 (US).

37 *Identity Theft Penalty Enhancement Act of 2004* 18 USC § 1001 (US)

38 United States Government Federal Trade Commission, *State Laws: Criminal* <www.ftc.gov> at 1 May 2008.

12.21 In the United Kingdom it is also an offence, with some exceptions, to obtain, disclose or procure the disclosure of personal data without the consent of the data controller.[39] This offence provision could be used to prosecute those who engage in identity theft. The *Identity Cards Act 2006* (UK) makes it an offence to possess or control false identity documents, including genuine documents that belong to another person.[40]

Other responses to identity theft

12.22 It has been argued that criminalising identity theft may be ineffective because it is difficult to detect[41] and prosecute successfully.[42] Other responses to identity theft can be divided into responses aimed at preventing identity theft and responses aimed at remedying its adverse effects after it has occurred.

12.23 Initiatives aimed at preventing identity theft generally aim to:

- educate individuals about how to minimise the risk of identity theft;[43]
- enhance the security features of identification documents so that they cannot be altered or forged; and
- strengthen the procedures used to authenticate the identity of individuals engaging in transactions with agencies or organisations.[44]

12.24 Initiatives aimed at minimising the harm of identity theft tend to focus on assisting victims of identity theft to remedy the adverse effects of the theft and to regain control over the use and disclosure of their personal information.

Identity theft and privacy laws

12.25 Identity theft represents a threat to privacy when it involves the theft or assumption of the identity of a living person. While it is appropriate to introduce laws

---

39 *Data Protection Act 1998* (UK) s 55.

40 *Identity Cards Act 2006* c 15 (UK) s 25.

41 D Solove, 'The Legal Construction of Identity Theft' (Paper presented at Symposium: Digital Cops in a Virtual Environment, Yale Law School, New Haven, 26–28 March 2004).

42 Ibid; N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 10.

43 The Office of the Privacy Commissioner has published guidance on ways to avoid identity theft. For example, see Office of the Privacy Commissioner, *Scanning 'Proof of Identity' Documents*, Information Sheet 20 (2007).

44 For example, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), and the rules issued under s 229 of the Act, describe the customer identity verification procedures that must be followed by a reporting entity that delivers to a customer a service that is designated by the Act. See, eg, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) pts 2, 7 and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1) 2007* (Cth) chs 4, 6–7.

that criminalise identity theft, privacy laws also can assist in preventing the theft of a person's identity and minimising the harm caused by identity theft after it has occurred. In this Report, the ALRC recommends a number of reforms with potential application to identity theft. These are considered below.

The model Unified Privacy Principles

12.26 A number of the model Unified Privacy Principles (UPPs) are relevant to the problem of identity theft. Some of these principles—such as those requiring personal information to be stored securely and those restricting the circumstances in which personal information can be disclosed—may assist in preventing identity theft by preventing the widespread dissemination of personal information.[45] Others—such as the principle requiring personal information to be accurate—may assist in minimising the harm caused by identity theft after it has occurred.[46] The privacy principles are discussed in detail in Part D.

Breach notification

12.27 One way to combat identity theft is to require agencies and organisations to notify individuals of any unintended or unauthorised disclosure of their personal information. This alerts individuals to the possibility that they may be at risk of identity theft and may assist them to take steps to prevent the theft of their personal information. Alternatively, it may assist them to detect promptly any theft of their personal information. In Chapter 51, the ALRC recommends that the *Privacy Act* be amended to include a Part on data breach notification, which would require an agency or organisation to notify the OPC and affected individuals of a data breach in certain circumstances.[47]

Publicly available information in electronic form

12.28 Information stored in electronic form can be easily accessed, searched and aggregated. In particular, the internet has changed the notion of the public domain. Online public records often contain a wealth of identifying information and there is concern that this information may be used to facilitate identity theft.[48] This issue is discussed in Chapter 11. The ALRC recommends that the OPC should develop and publish guidance on generally available publications available in an electronic form.[49]

12.29 In Chapter 67, the ALRC discusses the importance of early education on the impact of the internet on privacy. The ALRC recommends that, to promote awareness

---

45 See the 'Data Security' and 'Use and Disclosure' principles set out in the model Unified Privacy Principles at the beginning of this Report. A discussion of security in the online environment is contained in Ch 9.

46 See the 'Data Quality' and the 'Access and Correction' principles set out in the model Unified Privacy Principles at the beginning of this Report.

47 Rec 51–1.

48 See, eg, L Myers, 'Online Public Records Facilitate ID Theft', *MSNBC* (online), 5 February 2007, <www.msnbc.msn.com>.

49 Rec 11–1.

of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, and, in particular, privacy in the online environment, into school curricula. Further, the OPC, in consultation with the Australian Communications and Media Authority (ACMA), should ensure that specific guidance on the privacy aspects of using social networking sites is developed and incorporated into publicly available educational material.[50]

Unique multi-purpose identifiers

12.30 The use of unique multi-purpose identifiers enhances the ability of agencies and organisations to compile and aggregate large amounts of personal information about individuals. This information, however, may be implicated in identity theft. For example, it has been noted that the most valuable piece of identifying information for identity thieves in the United States is the Social Security Number. Social Security Numbers are the key to assuming another person's identity because 'they are used to match consumers with their credit histories and many government benefits'.[51] In Chapter 30, the ALRC discusses the significant privacy risks associated with unique multi-purpose identifiers. The ALRC recommends that, before an agency introduces a unique multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should conduct a privacy impact assessment.[52]

Credit reporting

12.31 In the United States, the *Fair Credit Reporting Act 1970* (US) contains provisions designed to assist victims of identity theft. For example, this Act enables a victim of identity theft to require that a credit reporting agency insert a 'fraud alert' on a credit information file.[53] Further, in some parts of the United States, victims of identity theft can request a 'freeze' on their credit information files.[54] These, and other ways in which the credit reporting provisions of the *Privacy Act* can address the problem of identity theft, are discussed in Chapter 57. In particular, the ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to prohibit for a specified period the disclosure by a credit reporting agency of credit reporting information about them without their express authorisation.[55]

---

50 Recs 67–4, 67–3.

51 President's Identity Theft Task Force, *Interim Recommendations* (2006), 2. See also the discussion of Social Security Numbers in President's Identity Theft Taskforce, *Combating Identity Theft—A Strategic Plan* (2007).

52 Rec 30–6.

53 A fraud alert is a statement that notifies prospective users of a credit report that the individual to whom it relates 'may be a victim of fraud, including identity theft': *Fair Credit Reporting Act 1970* 15 USC § 1681 (US) § 1681c–1.

54 See, eg, *California Civil Code* § 1785.11.2–1785.11.6. Placing a freeze on a credit information file prevents it from being accessed by potential creditors.

55 Rec 57–5.

12.32 Finally, in Chapter 56, the ALRC notes that children and young people are a common target for identity theft as they often have unblemished or non-existent credit records. The ALRC recommends that the new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals who the credit provider or credit reporting agency knows, or reasonably should know, to be under the age of 18 years.[56]

56 Rec 56–9.

Part C

Interaction, Inconsistency and Fragmentation

13. Overview: Interaction, Inconsistency and Fragmentation

Contents

Introduction

13.1 Part C considers how the *Privacy Act 1988* (Cth) interacts with other federal, state and territory laws, and identifies areas of fragmentation and inconsistency in the regulation of personal information. A number of issues related to inconsistency and fragmentation are considered in other Parts of this Report. For instance, the inconsistencies between the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) are considered in Part D, the fragmentation that results from the various exemptions under the *Privacy Act* is outlined in Part E, inconsistency and

fragmentation in the regulation of health information is discussed in Part H, and the interaction of the *Privacy Act* and telecommunications legislation is considered in Part J.

The costs of inconsistency and fragmentation

13.2 Chapter 14 discusses some specific problems caused by inconsistency and fragmentation. These problems include unjustified compliance burden, multiple privacy regulators, impediments to information sharing and issues related to government contractors.

13.3 The ALRC makes a number of recommendations throughout this Report directed at dealing with problems caused by inconsistency and fragmentation in privacy regulation. Perhaps the most significant of these recommendations is the adoption of the model Unified Privacy Principles (UPPs), any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act* at the federal, state and territory level.[1] In the ALRC's view, these recommendations will deal with many of the problems identified in Chapter 14.

Compliance burden and cost

13.4 The Terms of Reference for this Inquiry require the ALRC to consider 'the desirability of minimising the regulatory burden on business'. The ALRC received a large number of submissions that claimed that the proliferation and fragmentation of privacy laws have increased compliance burden and cost for both agencies and organisations. Others submitted, however, that there is little evidence of the existence or extent of any unwarranted compliance burden.

13.5 It was noted in submissions that inconsistency and fragmentation in privacy regulation are particularly problematic for organisations that operate in more than one Australian jurisdiction, and complicate the implementation of programs and services at a national level. While stakeholders focused on the financial costs of this complexity, costs can also include social costs, such as delays in the provision of health services.

13.6 Inconsistency and fragmentation in the regulation of personal information at the federal, state and territory level create an unjustified additional compliance burden. The ALRC's recommendations for reform, including those highlighted in this chapter, would help reduce compliance costs, including through the adoption of a single set of privacy principles at the federal, state and territory level, and a redraft of the *Privacy Act* to minimise its complexity.

Multiple regulators

13.7 Some industries are required to comply with multiple layers of privacy regulation, which are overseen by more than one regulator. In submissions to the

1 See Ch 3 and Rec 3–4.

Inquiry, it was noted that the lack of consistency of federal and state and territory privacy regimes leads to confusion about where and how to complain in the event of an interference with an individual's privacy. Other submissions identified advantages in having multiple privacy regulators.

13.8 The ALRC considers that it is preferable to have privacy regulators at the federal, state and territory level.[2] This ensures that people in each jurisdiction have a regulator they can approach for advice and to make a complaint. It also ensures that agencies and organisations have access to a regulator who is aware of their local circumstances and can provide advice and training on implementing the legislation. Further, industry-specific regulators, such as the Telecommunications Industry Ombudsman and the Banking and Financial Services Ombudsman, provide industry expertise that the Office of the Privacy Commissioner (OPC) cannot provide.

13.9 There is evidence to suggest that multiple privacy regulators can create problems for individuals, agencies and organisations. The ALRC makes a number of recommendations aimed at improving the operation of multiple privacy regulators. These recommendations include: the development of memorandums of understanding between the OPC and other bodies with responsibility for information privacy;[3] amending the *Privacy Act* to empower the Privacy Commissioner to delegate all or any of his or her complaint-handling powers;[4] and the development and publication of complaint-handling policies, enforcement guidelines and educational material that address the role and functions of the various bodies with responsibility for information privacy.[5]

Sharing information

13.10 In submissions to the Inquiry, a wide range of examples were provided to illustrate how inconsistent, fragmented and multi-layered privacy laws have prevented or impeded information sharing. For example, the ALRC heard numerous examples of agencies and organisations using 'because of the *Privacy Act*' as an excuse for not providing information. Stakeholders also noted that inconsistent, fragmented and multi-layered privacy laws can act as a barrier to information sharing between federal, state and territory government agencies. This was identified as a particular issue in the areas of child protection, service provision to vulnerable persons, law enforcement and medical research.

13.11 It is undesirable that inconsistent and fragmented privacy laws prevent appropriate information sharing. Information-sharing opportunities, which are in the public interest and recognise privacy as a right to be protected, should be encouraged. Rather than preventing appropriate information sharing, privacy laws and regulators

2 See Rec 17–2.
3 Recs 17–3 and 73–8.
4 Rec 49–3.
5 Rec 73–9.

should encourage agencies and organisations to design information-sharing schemes that are compliant with privacy requirements.

13.12 A number of the ALRC's recommendations are directed at achieving greater transparency in information-sharing arrangements. The ALRC recommends that agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses the sharing of personal information.[6] The ALRC also recommends the development and publication of a framework relating to cross-border sharing of personal information within Australia by intelligence and law enforcement agencies.[7]

Government contractors

13.13 The *Privacy Act* imposes obligations on agencies entering into contracts to provide services to, or on behalf of, the agency. The Act requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider or a subcontractor does not do an act or engage in a practice that would breach the IPPs.

13.14 The ALRC, reflecting the view of the majority of stakeholders that commented on this issue, has concluded that the *Privacy Act* provisions relating to Commonwealth contractors remain appropriate and effective. The ALRC notes that some stakeholders have commented that the provisions are unclear. While the ALRC does not share this view, the redraft of the *Privacy Act* recommended in Chapter 5 may deal with these concerns.

13.15 Some state and territory privacy regimes require organisations that provide contracted services to a state or territory government agency to be bound by the relevant state privacy principles for the purposes of the contract. Other state regimes provide that compliance with the state privacy regime is subject to outsourcing arrangements, or are silent on this issue.

13.16 There are concerns that state or territory government contractors, who are otherwise private sector organisations, may not be bound by the *Privacy Act* or equivalent standards when performing functions under state or territory contracts. In Chapter 14, the ALRC considers whether the *Privacy Act* should be amended to include a 'roll-back provision' to cover state contractors. In the ALRC's view, however, such a law would intrude too heavily on state and territory government business. Instead, the ALRC recommends that state and territory privacy legislation should include provisions relating to state and territory contractors.

---

6 Rec 14–1.
7 Rec 14–2.

Federal information laws

13.17 In Chapter 15, the ALRC considers how the *Privacy Act* interacts with a number of federal laws that regulate the handling of personal information. Matters addressed in the chapter include: consistent terms and definitions; the interrelationship between the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) (FOI Act) and the *Archives Act 1983* (Cth); secrecy provisions; and Part VIII of the *Privacy Act* (obligations of confidence).

Terms and definitions

13.18 Federal legislation other than the *Privacy Act* regulates the handling of personal information. Sometimes this legislation adopts different terms or definitions to those used in the *Privacy Act*. For example, the concept of 'personal information' is central to the regime established by the *Privacy Act*, but other federal legislation adopts different terms such as 'personal affairs' to describe similar information. The definitions of other terms used in the *Privacy Act* also sometimes differ from the same terms in other federal legislation.

13.19 The inconsistent use of terms and definitions in privacy legislation contributes to the complexity of privacy law and may increase compliance burden and cost. The Australian Government should ensure the consistency of definitions and key terms in federal legislation that regulates the handling of personal information. The ALRC acknowledges that there will be occasions, however, when other policy considerations will justify the use of terms or definitions that differ from those used in the *Privacy Act*.

Freedom of Information Act 1982 (Cth)

13.20 The interrelationship between the FOI Act and the *Privacy Act* is significant. The FOI Act and the *Privacy Act* both regulate the way in which information is handled, but the Acts have different objectives. Freedom of information legislation is concerned mainly with transparency in government and protects privacy only to the extent that it prevents the unreasonable disclosure of personal information, and allows an individual to access and correct personal information. In contrast, privacy legislation is focused primarily on data protection and provides for transparency only to the extent that it enhances the information privacy rights of individuals.

13.21 On 24 September 2007, following the release of the ALRC's Discussion Paper, *Review of Privacy* (DP 72), the then Attorney-General of Australia requested that the ALRC examine and report on the extent to which the FOI Act and related laws continue to provide an effective framework for access to information in Australia. It is the ALRC's view that many issues related to the interaction between the FOI Act and the *Privacy Act* should be considered as part of that review.

13.22 In Chapter 15, however, the ALRC does deal with access to, and correction of, personal information under the *Privacy Act* and the FOI Act. Both the FOI Act and the

IPPs enable individuals to access personal information about them and to correct or annotate that information if it is incorrect, incomplete, out-of-date or misleading. The rights provided by the *Privacy Act* are found in IPP 6 and IPP 7. The correction rights in the FOI Act are located in Part V and are dependent on the individual having been lawfully provided with the document under the FOI Act or otherwise. A number of stakeholders submitted that the overlap has created confusion for both agencies and the public.

13.23 The ALRC has considered various models for dealing with the overlap, and recommends that an individual's right to obtain access to, or correction of, his or her own personal information held by an agency should be dealt with under the 'Access and Correction' principle of the *Privacy Act*.

13.24 The ALRC has concluded that an individual's right to access his or her own personal information should still be subject to the limitations under the FOI Act. Individuals should not be able to obtain access to information under the *Privacy Act* that would be the subject of an exemption under the FOI Act. In the ALRC's view, however, an individual's right to correct his or her own personal information under the *Privacy Act* should no longer be subject to the limitations of the FOI Act. For example, an individual's right to correct their own personal information should not be subject to the limitation under the FOI Act that an individual must have been lawfully provided with the document.[8]

13.25 The ALRC has concluded that, for the time being, Part V of the FOI Act should be retained. The issue of whether the FOI Act should continue to regulate access to, and correction of, personal information, however, should be considered as part of the ALRC's review of the FOI Act and related laws.

Archives Act 1983 (Cth)

13.26 The *Archives Act* establishes the National Archives of Australia and provides for the preservation of the archival resources of the Commonwealth. It also creates an access regime whereby the public generally has a right of access to Commonwealth records that are more than 30 years old. The *Archives Act* provides some protection of information relating to the 'personal affairs' of any person, including a deceased person.

13.27 It was suggested by one stakeholder that amending the 'personal affairs' exemption to apply to 'personal information' would protect privacy better, and harmonise the *Archives Act* with both the *Privacy Act* and the FOI Act.[9] There was strong opposition to this amendment from other stakeholders. It was noted that the reference to 'personal affairs' in the exemption is an appropriate recognition of the different age and sensitivity of the information covered by the *Archives Act*, that such

8 These issues are also discussed in Ch 29.

9 'Personal affairs' is generally considered to be a narrower concept than 'personal information'.

an amendment would restrict needlessly access to records, and would increase the workload of officers making access decisions under the Act. The ALRC concludes that, in the absence of any identifiable problem in this area, the benefits in changing the exemption to refer to 'personal information' do not outweigh the disadvantages of such an amendment.

A single information Act?

13.28 One option for consideration is whether, given the significant overlap between the FOI Act and the *Privacy Act*, the two Acts should be consolidated into a single Act. A number of overseas jurisdictions have combined freedom of information and privacy legislation. Another option would be to consolidate the FOI Act, the *Privacy Act* and the *Archives Act* into a single Act. An example of such legislation is the *Information Act 2002* (NT).

13.29 There was little support among stakeholders for combining the *Privacy Act*, FOI Act and *Archives Act*. Stakeholders noted that the three Acts have different purposes, and that the ALRC should focus on the harmonisation of the Acts. In the ALRC's view, the benefits to be gained by combining the Acts do not outweigh the disadvantages occasioned by disturbing the current legislative framework.

A single regulator?

13.30 The ALRC has also considered the option of the same regulator administering the *Privacy Act* and the FOI Act. This is the case in the Northern Territory, and a number of overseas jurisdictions—for example, the Office of the Information and Privacy Commissioner for British Columbia, the Office of the Ontario Information and Privacy Commissioner, and the United Kingdom Information Commissioner's Office.

13.31 There was little support for this proposal. It was noted in submissions that the *Privacy Act* and the FOI Act have a different focus, and should be administered by two different regulators. Further, a number of stakeholders supported a separate body, such as a Freedom of Information Commissioner, to oversee freedom of information at the federal level.

13.32 The ALRC does not recommend the establishment of a single body to administer the *Privacy Act* and the FOI Act. In the ALRC's view, however, the Australian Government should establish a statutory office of the FOI Commissioner to oversee the administration of the FOI Act and these functions should be conferred on the Commonwealth Ombudsman.

13.33 The ALRC notes the Australian Government's election policy document *Government Information: Restoring Trust and Integrity* which sets out the Government's proposals for a restructure of freedom of information laws. These proposals include bringing together the functions of privacy protection and freedom of information in an Office of the Information Commissioner. While the ALRC does not recommend a single regulator to administer the *Privacy Act* and the FOI Act, the

ALRC notes that the Government's policy for an Office of the Information Commissioner is consistent with the ALRC's recommendations in this Report.

Secrecy provisions

13.34 Federal legislation contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office. Secrecy provisions usually are based on the need to preserve the secrecy of government operations in order for government to function effectively.

13.35 In DP 72, the ALRC noted that there was no support for having the *Privacy Act,* rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by agencies. The ALRC considers that it is appropriate that specific statutes include secrecy provisions designed to protect information, because secrecy provisions do not relate solely to personal information. They also protect other information, for example, commercial information, security details and operational information.

13.36 In the ALRC's view, however, secrecy provisions in federal legislation should be reviewed.[10] This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*. The need for such a review has been established by a number of inquiries.

Obligations of confidence

13.37 Part VIII of the *Privacy Act* (Obligations of confidence) applies where an agency or an employee of an agency (a 'confidant') is subject to an obligation of confidence to another person (a 'confider') in respect of personal information. Part VIII of the *Privacy Act* represents an extension of the law of confidentiality in that it extends the right to enforce a duty of confidentiality to the subject of the personal information, not just the confider.

13.38 The ALRC recommends that the confidentiality provisions contained in Part VIII of the *Privacy Act* be repealed.[11] The ALRC notes that the courts in the United Kingdom have developed the action for breach of confidence so that it now covers the disclosure of information that the defendant knows, or ought to know, is private because such disclosure is a wrongful invasion of privacy. In the ALRC's view, the common law of Australia should not follow the United Kingdom example of transforming breach of confidence in this way. This is discussed in detail in Part K.

13.39 The ALRC considers that, rather than extending the law of confidentiality, it is more appropriate to enact a statutory cause of action for a serious invasion of privacy. The cause of action will: apply to both agencies and organisations, unlike Part VIII which only applies to agencies; provide broader protection of privacy than that offered

10 Rec 15–2.
11 Rec 15–3.

by Part VIII; and offer a range of remedies.[12] The ALRC also notes that the provisions of Part VIII have never been used.

Required or authorised by or under law

13.40 Chapter 16 considers the meaning of the phrase 'required or authorised by or under law'. The chapter then examines a number of federal Acts that require or authorise acts and practices for the purposes of the *Privacy Act*. These laws include the *Census and Statistics Act 1905* (Cth), the *Corporations Act 2001* (Cth), the *Commonwealth Electoral Act 1918* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act). The interaction between these laws and the *Privacy Act* has been the subject of recent public debate.

The meaning of 'required or authorised by or under law'

13.41 An act or practice required or authorised by or under law is an exception to a number of the IPPs and the NPPs. The ALRC recommends that acts or practices that are required or authorised by or under law should be an exception to a number of the model UPPs.

13.42 There is a public expectation that governments are able to make laws to facilitate the handling of information in certain appropriate and necessary ways. The required or authorised by or under law exception reflects this expectation.

13.43 The scope of the exception, however, requires clarification. Submissions noted that the ambiguity in the operation of this exception can create uncertainty for individuals, agencies, organisations and privacy regulators. The ALRC discusses various methods to clarify the scope of the exception and suggests that clear references to the required or authorised by or under law exception be included in any future legislative provisions that intend to rely on the exception.

13.44 The ALRC has concluded that the exception should be clarified by amending the *Privacy Act* to provide that 'law' for the purposes of determining when an act or practice is required or authorised by or under law includes Commonwealth, state and territory Acts and delegated legislation; a duty of confidentiality under common law or equity (including any exceptions to such a duty); an order of a court or tribunal; and documents that are given the force of law by an Act, such as industrial awards.[13]

13.45 The ALRC also recommends that the OPC should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law.[14] This guidance should include a list of examples of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*.

---

12 See Recs 74–1 to 74–5.
13 Rec 16–1.
14 Rec 16–2.

Census and Statistics Act 1905 (Cth)

13.46 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act*. The census is regarded as the most important source of statistical information in Australia. The information from the census is used to produce statistical data for use by governments, as well as academics, industry, businesses and private individuals.

13.47 Stakeholders raised a number of issues concerning two recent developments in relation to the census—the retention for 99 years of name-identified information collected in the census, and a proposal to enhance the value of the census by combining it with future censuses and possibly other datasets held by the ABS. The ALRC does not make a recommendation in relation to these developments. In the ALRC's view, the *Privacy Act* and the *Census and Statistics Act* continue to provide adequate protection of personal information collected as part of the census.

Corporations Act 2001 (Cth)

13.48 Section 168 of the *Corporations Act* requires companies and registered schemes to maintain a register of members, and, if relevant, a register of option holders and a register of debenture holders. The *Corporations Act* also requires companies to allow anyone to inspect these registers.

13.49 A number of issues in relation to registers of members were raised in submissions. The ALRC does not, however, make any recommendations concerning the availability of registers of members. The ALRC notes the significant public interest in disclosure of those who have control or an interest in a company. Further, the *Corporations Act*, and regulations made under it, provide significant protection of personal information held on a register of members.

Commonwealth Electoral Act 1918 (Cth)

13.50 Part VI of the *Commonwealth Electoral Act* provides for the establishment of an electoral roll. It is compulsory for all eligible persons in Australia to maintain continuous enrolment on the Commonwealth electoral roll for the purposes of federal elections and referendums. The names and addresses of all electors on the Commonwealth electoral roll are available for public inspection in various formats specified under the Act.

13.51 A range of issues raised in submissions related to the handling of personal information held on the electoral roll. In particular, the ALRC heard concerns about the use of old electoral rolls for unauthorised purposes, such as direct marketing. The ALRC notes that if the exemption under the *Privacy Act* that applies to registered political parties and political acts and practices is not removed, the *Commonwealth Electoral Act* should be amended. This amendment should provide that prescribed individuals, authorities and organisations to whom the Australian Electoral Commission must give information from the electoral roll and certified lists of voters, must take reasonable steps to protect the information from misuse and loss and from

unauthorised access, modification or disclosure. Such information should also be destroyed or rendered non-identifiable if it is no longer needed for a permitted purpose.

13.52 The ALRC recommends that the Australian Electoral Commission and state and territory electoral commissions, in consultation with the OPC, state and territory privacy commissioners and agencies with responsibility for privacy regulation, develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purpose of the continuous update of the electoral roll.[15]

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

13.53 The AML/CTF Act is intended to enable individual businesses to minimise money laundering and terrorism financing risks. The Act sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person who provides 'designated services'. A large number of 'designated services' are listed in the Act, including opening an account, making a loan, and supplying goods by way of hire purchase.

13.54 The Act requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer. In addition, a reporting entity must give the Australian Transaction Reports and Analysis Centre (AUSTRAC) reports about suspicious matters, and must have and comply with an anti-money laundering and counter-terrorism financing program. Part 11 of the Act provides that the Australian Taxation Office and certain other 'designated agencies' may access AUSTRAC information. 'Designated agencies' include a large number of Australian Government agencies as well as some state and territory agencies. The Act requires designated agencies to comply with the IPPs in respect of AUSTRAC information.

13.55 The AML/CTF Act is the result of an extensive consultation process and has been the subject of a number of recent inquiries. The ALRC, therefore, restricts its consideration of the Act to issues raised in submissions to this Inquiry. The ALRC recommends that the statutory review of the AML/CTF Act mandated by s 251 of the Act should consider a number of matters, including whether reporting entities and designated agencies are handling personal information under the legislation appropriately.[16]

Interaction with state and territory laws

13.56 In Chapter 17, the ALRC considers how the *Privacy Act* interacts with state and territory privacy laws. State and territory laws are sometimes inconsistent with the

15 Rec 16–3.
16 Rec 16–4.

Privacy Act and with each other. Legislation regulates personal information at the federal level and in New South Wales, Victoria, Tasmania, the ACT and the Northern Territory. Queensland and South Australia have adopted administrative regimes for the management of personal information in their state public sectors. Western Australia does not have a legislative scheme to regulate personal information. State freedom of information legislation and public records legislation, however, provide some privacy protection.[17]

13.57 Further, legislation in New South Wales, Victoria and the ACT regulates health information in the public and private sectors. These Acts overlap substantially with the private sector provisions of the *Privacy Act*. Regulation of health information in other jurisdictions is restricted to public sector agencies or is the subject of codes and guidelines. Inconsistency and fragmentation in health privacy regulation is discussed in Part H.

Federal, state and territory regimes that regulate personal information

13.58 There is inconsistency in the coverage of the *Privacy Act* and the state and territory schemes. For example, state-owned corporations, ministers, universities and local governments are regulated under privacy regimes in some states and territories, but not others. The types of personal information regulated at the federal, state and territory level also differs. For example, employee records are excluded from the operation of the *Privacy Act*. Some state and territory privacy regimes, however, provide limited protection of employee records.

13.59 Although the IPPs, NPPs and privacy principles under state and territory privacy regimes are similar, they are not identical. The privacy regimes in some jurisdictions include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs.

13.60 The nature and functions of privacy regulators vary across the jurisdictions. For example, the *Privacy Act* and other federal legislation provide the Privacy Commissioner with a number of powers and functions, including powers to investigate and conciliate complaints, and approve and monitor privacy codes and guidelines. Although most states and territories have privacy regulators, their nature and functions vary widely. For example, the Privacy Committee of South Australia's powers and functions are limited when compared to the federal, New South Wales and Victorian privacy commissioners.

---

17 On 28 March 2007, the Information Privacy Bill 2007 (WA) was introduced into the Western Australian Parliament. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information by the public and private sectors in Western Australia. In May 2008, the Bill had been read for a second time in the Legislative Council.

13.61 The remedies available to individuals whose privacy rights are infringed can differ according to the jurisdiction in which the complaint is made. For example, the maximum amount of compensation that is payable for an interference with privacy differs across the states and territories.

13.62 As noted above, in Chapter 3 the ALRC recommends that the states and territories enact privacy laws that apply the model UPPs, any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act*, to regulate the public sector in that state or territory. Implementation of this recommendation will go a long way to address inconsistency in the regulation of personal information.

Privacy rules, codes and guidelines

13.63 In addition to the *Privacy Act* and state and territory legislation, various privacy rules, codes and guidelines regulate the handling of personal information. Sometimes privacy rules, codes and guidelines are required by legislation. Sometimes, however, particular industries or sectors choose to develop guidelines.

13.64 A number of stakeholders noted that if rules, codes and guidelines are not aligned with the *Privacy Act*, they can contribute to inconsistency and fragmentation. On the other hand, it was also noted that additional privacy rules, codes and guidelines can clarify sector-specific issues and provide more detailed protection for personal information where appropriate.

13.65 In the ALRC's view, when agencies and organisations are developing privacy rules, codes and guidelines, they should consult with the relevant body responsible for privacy for their industry or sector to ensure that the rules, codes or guidelines will interact and operate effectively with existing privacy laws.

Residential tenancy databases

13.66 Residential tenancy databases (RTDs) are also discussed in Chapter 17. RTDs are electronic databases operated by private companies that contain information about tenants, including their rental history. The purpose of such databases is to enable real estate agents to assess 'business risk' on behalf of the property owner. The listings on the database are based on information provided by real estate agents to the database operators. Listings are generally collected from across Australia and can be accessed nationally.

13.67 A number of inquiries have recognised the need for national consistency in the regulation of RTDs. As RTDs contain personal information, they are generally subject to the private sector provisions of the *Privacy Act*. They are also regulated by legislation in some states and territories. While the states and territories can regulate the actions of the lessors and agents in their jurisdictions, they lack the power to regulate effectively the RTD operators based in other jurisdictions.

13.68 Stakeholders raised a number of concerns about the operation of RTDs, including that: prospective tenants often will have little choice but to consent to a real estate agent passing information on to RTD operators; information stored on RTDs is sometimes inaccurate; and tenants sometimes have difficulties in finding out whether they are listed on RTDs. The ALRC also heard that inconsistent state and territory legislation in relation to RTDs causes a number of problems.

13.69 The states and territories should enact legislation that addresses the relationship between the agent and the tenant. Issues to be covered include informing the tenant of the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs.

13.70 Further, all RTD operators should be regulated by the *Privacy Act*, regardless of whether they are small business operators or whether they gain consent for the collection or disclosure of an individual's personal information. The ALRC does not recommend binding rules to regulate RTD operators, however, the Australian Government should continue to monitor the use and operation of RTDs in order to determine whether it should promulgate regulations under the *Privacy Act* to regulate RTD operators.

14. The Costs of Inconsistency and Fragmentation

Contents

Introduction

14.1 This chapter focuses on some specific problems caused by inconsistency and fragmentation in privacy regulation in Australia. The chapter first considers the compliance burden and cost caused by inconsistent privacy requirements across jurisdictions and sectors. Secondly, the problems caused when particular agencies and organisations are required to comply with multiple layers of privacy regulation overseen by more than one regulator are discussed. Thirdly, the chapter considers how inconsistent and fragmented privacy laws can result in reluctance by organisations and agencies to share information. Finally, the chapter outlines various issues related to government contractors.

Compliance burden and cost

14.2 The Terms of Reference for this Inquiry require the ALRC to consider 'the desirability of minimising the regulatory burden on business'. Business has identified

the pervasive nature of privacy requirements as an important contributor to the cumulative regulatory burden it faces.[1] The Australian Chamber of Commerce and Industry has reported that, in response to its 2004 Pre-Election Survey, 47.4% of Australian businesses polled considered that compliance with privacy requirements was a problem.[2]

14.3 The Taskforce on Reducing Regulatory Burdens on Business (the Regulatory Taskforce) heard that inconsistency in the areas of workplace surveillance, direct marketing and telemarketing laws, and having to supply information to multiple government agencies, contributed to compliance burdens and costs.[3] The Office of the Privacy Commissioner (OPC) review of the private sector provisions of the *Privacy Act* (OPC Review) was told that the lack of a single, national and comprehensive regime makes compliance more difficult and that the complexity of federal privacy laws (including the *Privacy Act* and the *Telecommunications Act 1997* (Cth)) contributes to compliance costs.[4] The Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (the Senate Committee privacy inquiry) also heard about compliance burden and cost.[5]

14.4 The Regulatory Taskforce noted that nationally consistent privacy laws would reduce compliance costs for business,[6] and recommended that the Australian Government ask the Standing Committee of Attorneys-General (SCAG) to endorse national consistency in all privacy-related legislation.[7] In its response, the Australian Government stated that:

> The Australian Government agrees to the recommendation and supports the goal of national consistency in privacy-related legislation. At the April 2006 meeting of the Standing Committee of Attorneys-General, Attorneys-General agreed to establish a working group to advise Ministers on options for improving consistency in privacy regulation, including workplace privacy.[8]

14.5 The Productivity Commission report, *Performance Benchmarking of Australian Business Regulation*, found that there was evidence that significant differences in compliance costs exist across jurisdictions. The Productivity Commission concluded

---

1 See, eg, Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 54.

2 Australian Chamber of Commerce and Industry, *Submission to the Taskforce on Reducing Regulatory Burdens on Business*, 1 November 2005, 5.

3 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 53–57.

4 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 36–37, 66.

5 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.149]–[4.154].

6 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), [4.151].

7 Ibid, rec 4.47.

8 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

that the benchmarking of regulatory burdens across jurisdictions could shed light on where and how such differences might be reduced and increase government accountability for the design, administration and enforcement of regulation.[9]

Do privacy laws cause an unjustified compliance burden?

14.6 The ALRC received a large number of submissions that claimed that the proliferation and fragmentation of privacy laws have increased compliance burden and cost for both agencies and organisations.[10] In particular, stakeholders noted that state health privacy legislation and workplace surveillance laws are creating complexity and unjustified compliance costs.[11] It also was noted that compliance burden is a particular issue for small businesses that are required to comply with the *Privacy Act*.[12]

14.7 In the Office of the Privacy Commissioner's (OVPC) view, there is little evidence of the existence or extent of any compliance burden. It noted, however, that compliance burden is most likely to be a problem for organisations that do not have the resources to obtain advice and training about their privacy obligations, especially where they are working in an area that intersects with multiple privacy regimes. This often has an impact on service providers, especially where they receive joint Commonwealth-state funding.[13]

14.8 The OPC submitted that, in many areas, the compliance obligations are proportionate and appropriate to public expectations. It noted, for example, that the *Privacy Act* requires agencies and organisations to take actions that are 'reasonable' to

---

9 Australian Government Productivity Commission, *Performance Benchmarking of Australian Business Regulation* (2006), 156. The Productivity Commission has since announced that it will undertake a series of annual reviews of regulatory burdens on business under Australian Government regulation. It is not clear when privacy regulation will be reviewed: Productivity Commission, *Annual Review of Regulatory Burdens on Business—Primary Sector*, Productivity Commission Circular, 28 February 2007.

10 See, eg, Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Telstra, *Submission PR 185*, 9 February 2007; Australian Health Insurance Association, *Submission PR 161*, 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Australian Retailers Association, *Submission PR 131*, 18 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Australasian Compliance Institute, *Submission PR 102*, 15 January 2007; Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007; D Antulov, *Submission PR 14*, 28 May 2006.

11 See, eg, Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007. A Standing Committee of Attorneys-General (SCAG) working party is currently considering workplace privacy: see Chs 1 and 2. SCAG recently agreed to the working group developing a minimum model for nationally consistent workplace privacy regulation: Standing Committee of Attorneys-General, *Communiqué*, 28 March 2008.

12 Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; Australasian Compliance Institute, *Submission PR 102*, 15 January 2007. See also Ch 39.

13 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

fulfil obligations relating to notice requirements, data quality and data security. What is considered 'reasonable' is contextual, and may depend on the entity's size and activities. The OPC stated, however, that it recognised that compliance costs escalate where entities must comply with multiple layers of privacy regulation, and suggested that

> the solution may be to resolve questions of jurisdiction. For example, by clarifying that the *Privacy Act* 'covers the field' of the private sector to the exclusion of other jurisdictions' privacy legislation. In other cases, governments and regulators may work together to promote greater consistency between regulations and administrative procedures, without disrupting existing regulatory frameworks.[14]

14.9 Inconsistency and fragmentation in privacy regulation are a problem for organisations that operate in more than one Australian jurisdiction. For example, the OPC Review was told by one organisation that operates nationally that

> a single piece of personal information may be subject to two or more … legislative regimes at one time, creating conflicting obligations, different obligations or more onerous obligations in respect of the whole or parts of that same piece of information.[15]

14.10 The OPC Review also cited an instance where a national medication service operating via a call centre had to read different statements to obtain consent depending on the location of the individual (and the law that applied in that state or territory).[16] The Regulatory Taskforce also noted that this was an issue in the context of different laws relating to direct marketing.[17]

14.11 National organisations making submissions to this Inquiry noted that the main issue for them is compliance burden and cost.[18] In particular, differences in rules governing acceptable calling times for telemarketers, and state and territory laws dealing with the privacy of employee records, were highlighted as problematic.[19] State health privacy legislation also is creating problems for national organisations.[20] The OPC submitted that in some cases these problems are

> an inevitable consequence of large-scale operations across a federal system, which national organisations are often better equipped to deal with due to their size. In

---

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

15 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 40.

16 Ibid, 66.

17 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 54.

18 See, eg, AAMI, *Submission PR 147*, 29 January 2007; Australian Retailers Association, *Submission PR 131*, 18 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; AXA, *Submission PR 119*, 15 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Australasian Compliance Institute, *Submission PR 102*, 15 January 2007; D Antulov, *Submission PR 14*, 28 May 2006.

19 Telstra, *Submission PR 185*, 9 February 2007; AAMI, *Submission PR 147*, 29 January 2007.

20 AAMI, *Submission PR 147*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

> particular sectors, including health, greater consistency in regulation would clarify obligations and may facilitate the implementation of interstate and national initiatives.[21]

14.12 Multi-layered regulation of personal information complicates the implementation at a national level of programs and services. This is an issue in the health sector, where multi-layered regulation creates a compliance burden and affects quality in the health care and health and medical research sectors.[22] The Australian Bureau of Statistics stated that complex and overlapping legal requirements across jurisdictions make it difficult to collect and use for statistical purposes state and territory administrative data.[23]

14.13 The National Transport Commission, an independent body established under federal legislation to maintain uniformity in regulatory transport reforms, submitted that inconsistent privacy laws have made national reforms to transport unnecessarily complex. Inconsistent privacy laws have often required tailoring legislation and policy in order to maintain the effectiveness of legislative privacy requirements in each Australian state and territory.[24]

Quantifying the compliance burden

14.14 Stakeholders submitted that inconsistent privacy laws create a compliance burden in the following areas: monitoring changes to the law; staff training; changing internal policies and procedures; rewriting privacy policies and consumer information; and lost business due to a consumer perception of a lack of service.[25] The Australasian Compliance Institute noted that many of these costs are ongoing, due to continuous changes in federal, state and territory legislation.[26]

14.15 The Australasian Compliance Institute also noted that compliance costs often are passed on to the consumer.[27] These costs are not always financial. For example, the NHMRC submitted that the multi-layered level of privacy laws sometimes will prevent information exchange for the purpose of medical research. This can compromise clinical care, quality assurance and related activities because: access to essential health information is impaired; significant research is not approved or submitted for approval;

---

21 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
22 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.
23 Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007.
24 National Transport Commission, *Submission PR 416*, 7 December 2007.
25 See, eg, Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007; Australian Chamber of Commerce and Industry, *Submission PR 219*, 7 March 2007; AAMI, *Submission PR 147*, 29 January 2007; Australasian Compliance Institute, *Submission PR 102*, 15 January 2007.
26 Australasian Compliance Institute, *Submission PR 102*, 15 January 2007.
27 Ibid.

additional requirements are imposed on some research that reduce its scientific rigour; and excessive administrative effort and costs are incurred.[28]

ALRC's view

14.16 Some of the compliance burden imposed by the *Privacy Act* is justified. The *Privacy Act* was enacted to implement Australia's obligations relating to privacy under the *International Covenant on Civil and Political Rights* as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[29] It was enacted, therefore, to protect a fundamental human right—the right of an individual to privacy.

14.17 The compliance requirements under the *Privacy Act* are minimal when compared to comparable schemes in Europe that often include an expensive registration requirement. The Act also does not have extensive reporting requirements such as under the *Corporations Act 2001* (Cth). Further, as noted by the OPC, the Act can take account of an agency or organisation's size and activities. The ALRC also notes that the OPC is available to provide guidance free of charge to agencies and organisations.

14.18 In the ALRC's view, however, inconsistency and fragmentation in the regulation of personal information at the federal, state and territory level does create an unjustified compliance burden. Time and money can be spent identifying sources of privacy obligations and complying with disparate laws and inconsistent privacy standards in different jurisdictions. This problem is acute when implementing programs and services by agencies and organisations at a national level. The costs associated with this burden are both financial and social.

14.19 The ALRC makes a number of recommendations throughout this Report that are intended to minimise inconsistency and fragmentation, and streamline the regulation of personal information. For example, the ALRC recommends: the amendment of the *Privacy Act* to provide that it is intended to apply to the exclusion of state and territory laws dealing with the handling of personal information by organisations; the adoption of the model Unified Privacy Principles (UPPs) at the federal, state and territory level; and a redraft of the *Privacy Act* to minimise its complexity.[30] The ALRC also makes a number of recommendations to clarify the interaction of different laws that regulate the handling of personal information, particularly laws that regulate the health sector, credit reporting, and the telecommunications industry.[31]

---

28 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007. See also CSIRO, *Submission PR 176*, 6 February 2007.

29 See discussion in Chs 1, 3.

30 See Chs 3, 5.

31 See Parts G, H, J.

14.20 The ALRC also recommends a greater emphasis on the OPC's educative role. For example, the ALRC recommends that the OPC develop and publish guidance about the interaction of the *Privacy Act* with other federal, and state and territory laws that regulate the handling of personal information. Parts F and J also include a number of recommendations designed to promote greater cooperation between privacy regulators and other bodies with responsibility for privacy.

Multiple regulators

14.21 Some industries are required to comply with multiple layers of privacy regulation overseen by more than one regulator. This has been identified as an issue in the telecommunications industry[32] and the financial services sector. For example, bank customers with privacy complaints may choose to lodge a complaint with the Banking and Financial Services Ombudsman (BFSO) or the OPC.

14.22 It has been noted that industry ombudsmen and the OPC may take opposing views in relation to the same privacy complaint. Concerns were expressed to the OPC Review about the lack of clarity in the respective complaint-handling responsibilities of the federal and New South Wales privacy commissioners,[33] and that consumers may not know to which regulator to complain, or which law applies to their matter.[34]

Submissions and consultations

14.23 In submissions to this Inquiry, stakeholders noted that the lack of consistency of federal and state and territory privacy regimes leads to confusion about to whom to complain, and how to complain.[35] They noted that it would be useful to have a 'one-stop shop' for complaint handling.[36]

14.24 A number of organisations reported that multiple regulators contribute to compliance cost by increasing the number of 'compliance activities' required each year and the slower resolution of privacy complaints.[37]

---

32 See discussion in Part J and Telstra, *Submission PR 185*, 9 February 2007; Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, 9.

33 Private Health Insurance Ombudsman, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 14 December 2004, 1.

34 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 68.

35 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006.

36 Telstra, *Submission PR 185*, 9 February 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007.

37 Telstra, *Submission PR 185*, 9 February 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007. See also Australian Chamber of Commerce and Industry, *Holding Back the Red Tape Avalanche: A Regulatory Reform Agenda for Australia* (2005).

14.25 Privacy regulators also noted difficulties. The OVPC submitted that there will be cases where privacy regulators cannot agree on which privacy law applies.[38] The OPC emphasised that lack of consistency in legislation is often the primary source of the problem, rather than the existence of more than one regulator.[39] The OPC observed, however, that the existence of multiple regulators at the federal, state and territory level raises three concerns:

> First, it can be difficult for individuals to understand their rights, and know how to enforce them. Second, organisations may bear increased compliance costs by having to obey multiple sets of regulations. Third, this may lead to unnecessary duplication of effort and resource expenditure by regulators.[40]

14.26 The OPC considered that the existence of multiple regulators in one sector presents the potential risks of forum shopping, inefficient use of resources, and inconsistent outcomes. In the OPC's view, however, these issues could be overcome by

> creating memoranda of understanding, harmonisation of complaint-handling procedures and legislative interpretation, and appropriate referral mechanisms. Where the source of these problems is inconsistent legislation, clarifying the scope of each regulator's jurisdiction could help to avoid such risks, provided this does not lead to gaps in regulatory coverage.[41]

14.27 The Australian Privacy Foundation submitted that having more than one regulator results in 'peer review', which can contribute to the maintenance of high standards and a consumer focus. It noted, however, that it is essential that multiple privacy regulators establish a good working relationship.[42]

14.28 The need for regulators with expertise in certain industry sectors was noted in other submissions. For example, the NHMRC submitted that health privacy issues require the attention of regulators who are expert in privacy and also have specific expertise in the health services and health and medical research sectors.[43] The Australian Bankers' Association noted that the majority of the few privacy-related complaints the BFSO receives are part of wider banking complaints. It is therefore convenient for the customer to have the dispute dealt with by the one body, particularly as the OPC would not have the power to determine the banking aspects of the dispute.[44]

---

38 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

39 The OPC noted the inconsistency between the *Privacy Act* and NSW health privacy legislation: see Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007 and Part H.

40 Ibid.

41 Ibid.

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

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

44 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

ALRC's view

14.29 There are several benefits in having multiple regulators that are responsible for privacy. It is preferable to have privacy regulators at the federal, state and territory level as it ensures that citizens in each jurisdiction have a regulator they can approach for advice and to make a complaint. Similarly, organisations that are subject to local privacy laws have access to a state and territory regulator who is aware of their circumstances and can provide advice and training on implementing the legislation.[45]

14.30 Further, industry-specific regulators, such as the BFSO and the Telecommunications Industry Ombudsman, play an important role in the regulation of personal information handling as they provide industry expertise that the OPC does not possess. Industry-specific regulators also reduce the volume of privacy complaints that would otherwise be made to the OPC, freeing the OPC's resources for other functions.

14.31 Another potential benefit is peer review and the promotion of high standards of performance. This will occur when privacy regulators interpret a single set of privacy principles. Transparency also can be promoted by publishing decisions and guidance on the operation of the principles.

14.32 The ALRC also accepts, however, that there is evidence to suggest that multiple privacy regulators can create confusion for individuals when making complaints, and for organisations and agencies when seeking advice. Further, it can create a compliance burden for businesses and result in the inefficient use of privacy regulators' resources.

14.33 The ALRC therefore makes a number of recommendations aimed at achieving greater cooperation between privacy regulators. Issues related to multiple regulators at the federal, state and territory level are discussed in more detail in Chapter 17—'Interaction with State and Territory Laws'. In that chapter, the ALRC recommends that state and territory privacy legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

14.34 The ALRC also recommends that the OPC develop and publish memorandums of understanding with each of the bodies with responsibility for information privacy in Australia, including industry-specific dispute resolution bodies and state and territory bodies with responsibility for privacy. These memorandums of understanding should outline:

- the roles and functions of each of the bodies;
- when a matter will be referred to, or received from, each of the bodies; and

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

- processes for consultation between the bodies when issuing public interest determinations, temporary public interest determinations and codes, and for the development and publication of joint guidance.

14.35 Other relevant recommendations include amendment of the *Privacy Act* to empower the Privacy Commissioner to delegate all or any of the powers in relation to complaint handling conferred on the Commissioner by the Act;[46] and the development and publication of complaint-handling policies, enforcement guidelines and educational material that addresses the role and functions of the various bodies with responsibility for information privacy.[47]

Sharing information

14.36 Inconsistent, fragmented and multi-layered privacy regulation can contribute to confusion about how to achieve compliance with privacy regulation. This, in turn, can result in reluctance by agencies and organisations to share information.[48]

14.37 The OPC submitted that some obstacles to appropriate information sharing between agencies and organisations may arise either from misapplication or a 'risk-averse' interpretation of privacy laws.[49] The ALRC heard numerous examples of agencies and organisations using 'because of the *Privacy Act*' as an excuse for not providing information.[50] In many cases, however, the *Privacy Act 1988* (Cth) would not have prohibited the sharing of the information. For example, a member of the public reported that:

> My daughter attends a childcare centre in my local area. One day, the carer commented on how well she was playing with a special friend. When I asked who the

---

46 See Ch 49.

47 See Chs 17, 73.

48 This phenomenon is not peculiar to Australia. See, eg, M Apuzzo, 'Privacy Law Confusion Impedes Sharing', *The Daily Texan* (online), 14 June 2007, <www.dailytexanonline.com>; T Tsunetsugu and A Nakamura, 'Personal Information Law Taken Too Literally', *Daily Yomiuri*, 7 April 2007, <www.yomiuri.co.jp>; 'Stop Using the Privacy Act as an Excuse to Do Nothing', *New Zealand Herald* (online), 6 May 2007, <www.nzherald.co.nz>. On 25 October 2007, the Prime Minister of the United Kingdom asked the United Kingdom Government Information Commissioner, Richard Thomas, and Dr Mark Walport, Director of the Wellcome Trust, to carry out an independent review of the use and sharing of personal information in the public and private sectors. The review will consider whether there should be any changes to the way the *Data Protection Act 1998* (UK) operates. The review also will make recommendations on how data-sharing policy should be developed in a way that ensures proper transparency, scrutiny and accountability. A report of the review will be published in the first half of 2008: United Kingdom Government Ministry of Justice, *Data Sharing Review Consultation* (2007) <www.justice.gov.uk> at 4 February 2008.

49 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Government of South Australia, *Submission PR 565*, 29 January 2008; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.

50 See, eg, Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also I Cuncliffe, *Submission to Senate Legal and Constitutional Affairs Committee Inquiry into the Privacy Act*, 22 February 2005.

> special friend was, I was advised that the name of the child, even the first name, couldn't be released to me due to the provisions of the *Privacy Act*. This is crazy.[51]

14.38 The complexity of privacy laws can act as a barrier to information sharing between federal, state and territory agencies,[52] and between agencies and organisations.[53] For example, the OVPC submitted that information sharing can be problematic where federal agencies such as Centrelink, the Australian Taxation Office (ATO) and the Electoral Commissioner want bulk access to state datasets because:

- some states have no privacy law and so provide the information;
- other states have privacy or other legislative provisions restricting disclosure to jurisdictions that do not have adequate privacy protection in place; and
- the Commonwealth can override privacy protection in state legislation to collect and use datasets in ways not authorised under, or anticipated by, state law.[54]

14.39 The Queensland Government noted that there is some evidence of inconsistency in privacy regulation affecting national schemes involving the participation of state and territory agencies.

> For example, Queensland Transport's participation in the National Exchange of Vehicle Driver Information System (NEVDIS). Queensland Transport has experienced resistance from counterpart agencies in other states with privacy legislation regarding sharing of information.[55]

14.40 A number of stakeholders noted that a failure to share information because of privacy concerns can impede investigations by law enforcement bodies;[56] prevent health studies;[57] make it impossible to track customers who have stolen rental goods;[58] prevent former 'wards of the state' reconnecting with their family members;[59] and

---

51 National Privacy Phone-In Comment No 607, June 2006.

52 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007.

53 See, eg, Queensland Government, *Submission PR 242*, 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Insolvency and Trustee Service Australia, *Submission PR 123*, 15 January 2007.

54 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

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

56 Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007. See also CrimTrac, *Submission PR 158*, 31 January 2007; Independent Pricing and Regulatory Tribunal of New South Wales, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency: Other Industries—Final Report* (2006), 225–226.

57 Australian Nuclear Veterans Association Inc, *Submission PR 324*, 24 September 2007.

58 J Tozzi-Condivi, *Submission PR 438*, 10 December 2007.

59 P Slatterie, *Submission PR 329*, 3 October 2007.

result in decisions in family law matters being made without a complete picture of family circumstances.[60] Further, a failure to share information can have grave consequences, such as the death of children who are at risk of abuse and neglect.[61]

14.41 The complexity of privacy laws is a particular issue in the context of service provision to vulnerable people.[62] The Community Services Ministers' Advisory Council (CSMAC) noted that the range of differing privacy regimes across Australia creates problems for information exchange between jurisdictions, including in the critical area of child protection, where state and territory specific legislation applies. Issues also arise in relation to information exchange within jurisdictions, where some non-government welfare organisations are subject to the *Privacy Act*, and state and territory agencies must comply with state and territory regimes. CSMAC noted that this inconsistency creates difficulties in relation to the development of memorandums of understanding and other protocols governing the exchange of information.[63]

14.42 Real or perceived restrictions on information sharing by agencies also can have an impact on business. The Regulatory Taskforce noted that barriers to sharing data between different agencies can mean that businesses often are required to supply the same information to multiple agencies, which can contribute to compliance cost.[64]

14.43 Inconsistency and fragmentation in privacy laws should not prevent appropriate information sharing. Information sharing opportunities, which are in the public interest and recognise privacy as a right to be protected, should be encouraged. Rather than preventing appropriate information sharing, privacy laws and regulators should encourage agencies and organisations to design information-sharing schemes that are compliant with privacy requirements or, where necessary, seek suitable exemptions or changes to legislation to facilitate information-sharing projects.

14.44 The ALRC makes a number of recommendations in relation to information sharing throughout this Report. Perhaps the most significant recommendation is the adoption of the model UPPs, any relevant regulations that modify the application of the UPPs, and key definitions at the federal, state and territory level.[65] Many of the real

---

60 Family Law Council, *Submission PR 269*, 28 March 2007.

61 A number of inquiries have considered this issue: see, eg, M Palmer, *Report of the Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau* (2005) Report to the Australian Government Minister for Immigration and Multicultural Affairs. See also Confidential, *Submission PR 327*, 28 September 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171*, 5 February 2007; Community Services Ministers' Advisory Council, *Submission PR 47*, 28 July 2006.

62 D Bowman, *Submission PR 330*, 19 October 2007; Confidential, *Submission PR 326*, 28 September 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171*, 5 February 2007; Community Services Ministers' Advisory Council, *Submission PR 47*, 28 July 2006.

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

64 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 56.

65 See Ch 3.

and perceived impediments to information sharing would be removed if the federal, state and territory public sectors and the private sector were required to comply with the same set of privacy principles. Adoption of the same privacy principles also would simplify the task of developing information-sharing protocols and memorandums of understanding. Other relevant recommendations include:

- redrafting the Act to achieve greater logical consistency, simplicity and clarity;[66]
- amending the 'Use and Disclosure' principle to permit the use and disclosure of a person's information for a secondary purpose where there is a threat to a person's life, health or safety that is serious (even if not necessarily imminent);[67]
- the inclusion of a new exception to allow the sharing of personal information (including sensitive information) for the purposes of non-medical research;[68] and
- the adoption of provisions that allow public interest determinations and temporary public interest determinations in state and territory laws regulating the public sectors.[69]

Education

14.45 Submissions to the Inquiry have established that many agencies and organisations are not aware of, or do not understand, their obligations under the *Privacy Act* and state and territory privacy laws. This can have a 'chilling effect' on information sharing.

14.46 The NSW Independent Pricing and Regulatory Tribunal (IPART) identified similar issues in its report, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency*. IPART recommended that the NSW Government provide guidance to agencies on privacy requirements affecting information sharing between agencies.[70] In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the OPC provide further guidance to agencies and organisations on privacy requirements affecting information sharing.[71]

---

66 Rec 5–2.
67 Rec 25–3.
68 See Rec 65–2.
69 See Rec 3–4.
70 Independent Pricing and Regulatory Tribunal of New South Wales, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency: Other Industries—Final Report* (2006), 228.
71 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 11–1.

Submissions and consultations

14.47 A number of stakeholders, including the OPC,[72] supported this proposal.[73] The Centre for Law and Genetics submitted that:

> Privacy must not promote a culture of secrecy, particularly as e-health develops with a capacity for beneficial transmission of personal health information. This Proposal will hopefully promote information sharing in a responsible, ethical and professional fashion within the overriding UPPs and developed contextual rules.[74]

14.48 The National Health and Medical Research Council (NHMRC) also supported the proposal. It noted that the recommended *Privacy (Health Information) Regulations* will need to be supported by health-specific guidance on privacy requirements affecting information sharing in health care contexts and in health and medical research.[75]

14.49 Centrelink and the Australian Government Department of Human Services submitted that such guidance would be beneficial, but noted that it will need to take into consideration confidentiality provisions that also may protect personal information.[76]

14.50 The Australian Government Department of Human Services submitted that the guidance also should deal with data-matching. The Department noted that much of the information sharing and data-matching undertaken by the agencies within the Human Services portfolio is undertaken pursuant to confidentiality provisions and to that extent would fall outside the OPC's responsibility. Additionally, legislation that deals with data-matching based on tax file numbers is the responsibility of the Minister for Families, Housing, Community Services and Indigenous Affairs. The Department submitted that the proposal may create a lack of clarity and accountability in relation to responsibilities regarding information sharing and data-matching.[77]

14.51 The School of Public Health at the University of Sydney submitted that the OPC's guidance should give due regard to the potential cost and privacy benefits of routine linkage of information and the provision of routine de-identified datasets to

---

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

73 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 536*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

74 Centre for Law and Genetics, *Submission PR 497*, 20 December 2007.

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

76 Australian Government Centrelink, *Submission PR 555*, 21 December 2007. See also Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

77 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

researchers and organisations concerned with the monitoring and improvement of health and health services.[78]

14.52 The OVPC submitted that the production of guidance alone does not provide adequate privacy protection. It submitted that the *Privacy Act* and state and territory privacy legislation should include rules about matters such as data-matching, similar to Part X of the *Privacy Act 1993* (NZ).[79]

ALRC's view

14.53 The ALRC notes that information sharing already is the subject of guidance published by the OPC, such as the *Plain English Guidelines to Information Privacy Principles* and *Guidelines to the National Privacy Principles*.

14.54 Rather than making a separate recommendation for guidance, in the ALRC's view, the OPC should consider including some additional matters in existing guidance. For example, the guidance could explain: how the privacy principles operate to allow or prevent the sharing of information in certain circumstances; when a public interest determination, temporary public interest determination or a code will be appropriate; when a privacy impact assessment should be prepared; and on the development of memorandums of understanding and protocols in relation to information-sharing schemes.

14.55 This guidance could be prepared in consultation with other bodies with responsibility for information privacy, including state and territory privacy regulators and industry-specific dispute resolution schemes.[80] The guidance should note that agencies and organisations may be subject to confidentiality provisions under federal, state and territory legislation, and that a body other than the OPC may be responsible for the administration of those provisions.

14.56 The ALRC notes the various issues raised by stakeholders in relation to data-matching. In Chapter 10, the ALRC discusses data-matching by agencies and organisations, and recommends that the OPC provide further guidance to organisations on the implications of data-matching.[81]

Guidelines and protocols

14.57 In DP 72, the ALRC proposed that, in the interest of greater transparency, agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses

78 School of Public Health—University of Sydney, *Submission PR 504*, 20 December 2007.
79 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
80 See Rec 17–3.
81 See Rec 10–4.

the sharing of personal information; and, where appropriate, publish other documents (including memorandums of understanding and ministerial agreements) relating to the sharing of personal information.[82]

Submissions and consultations

14.58 A number of stakeholders supported this proposal.[83] For example, the ATO submitted that the ALRC's approach would assist information sharing activities across agencies and promote consistency, awareness of obligations, and a more collaborative approach. The ATO also noted that it already has a number of memorandums of understanding with Australian Government and state government agencies with which it regularly shares information.[84]

14.59 The Queensland Government supported the proposal, provided the publication of such policies does not hinder the intent or purpose of that information sharing.[85] Other stakeholders noted that the publication of documentation relating to the sharing of information could be subject to secrecy provisions and confidentiality considerations.[86]

14.60 The Australian Federal Police (AFP) supported the proposal on the basis that there would be appropriate exemptions for operationally sensitive matters—for example, police methodology.[87] The Australian Government Department of Human Services supported the proposal, but noted that it may not be appropriate to divulge some business processes relating to fraud and compliance.[88]

14.61 Privacy NSW supported the proposal, but suggested that it should apply more broadly to any derogation from the UPPs. It submitted that complainants sometimes find out, after bringing their complaint, that the agency was permitted by law, a public interest direction,[89] or a code to engage in the conduct giving rise to the complaint, including the sharing of information between agencies. Privacy NSW submitted that this information should be made apparent to the individual at the time of collection or

---

82 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 11–2.

83 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; Confidential, *Submission PR 536*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

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

85 Queensland Government, *Submission PR 490*, 19 December 2007.

86 Medicare Australia, *Submission PR 534*, 21 December 2007; Confidential, *Submission PR 448*, 11 December 2007.

87 Australian Federal Police, *Submission PR 545*, 24 December 2007.

88 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

89 A public interest direction under the *Privacy and Personal Information Protection Act 1998* (NSW) is similar to a public interest determination under the *Privacy Act 1988* (Cth).

at the time of the intended secondary use or disclosure so that individuals do not bring a complaint about a matter that is lawful.[90]

ALRC's view

14.62 There is a public interest in the subject of the personal information and the public, where appropriate, knowing how agencies share personal information. The 'Notification' and 'Openness' principles require agencies to divulge when they may use or disclose personal information. These, however, do not require an agency to communicate how personal information will be shared.

14.63 Legislation, codes and public interest determinations that provide for information-sharing programs will not always set out clearly how agencies should implement those programs and protect personal information. Agencies that are required or authorised by legislation, a code or a public interest determination to share personal information, therefore, should develop and publish documentation that addresses the sharing of such information. This documentation may include guidance to assist officers to implement an information-sharing scheme, and protocols that detail how an agency can share information in compliance with privacy requirements.

14.64 Agencies often prepare documents that deal with information sharing. Ministerial agreements to share information and memorandums of understanding between agencies are examples of such documents. In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the NHMRC considered the legislative scheme establishing the National Criminal Investigation DNA Database—a national DNA database administered by the CrimTrac agency. To achieve greater transparency, the ALRC and AHEC recommended that the Commonwealth, states and territories publish all ministerial agreements for sharing genetic information required under the scheme,[91] as well as protocols for interjurisdictional matching.[92]

14.65 In the interest of greater transparency, agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses the sharing of personal information; and where appropriate, publish other documents (including memorandums of understanding and ministerial agreements) relating to the sharing of personal information.

---

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

91 Some state crimes legislation provides for the responsible minister in that state to enter into an arrangement with an Australian Government minister or with CrimTrac to provide for the transmission of information recorded in a state DNA database system to form part of the National Criminal Investigation DNA Database: see, eg, *Crimes (Forensic Procedures) Act 2000* (NSW); *Crimes Act 1958* (Vic); *Criminal Law (Forensic Procedures) Act 2007* (SA).

92 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 40–4.

14.66 The ALRC notes stakeholders' concerns that it may not always be possible to publish this documentation. The ALRC accepts that it will not always be appropriate to publish this documentation, particularly where the personal information is protected by secrecy provisions or confidentiality, or the publication would reveal operationally sensitive information.

Recommendation 14–1 Agencies that are required or authorised by legislation, a code or a Public Interest Determination to share personal information should, where appropriate, develop and publish documentation that addresses the sharing of personal information; and publish other documents (including memorandums of understanding and ministerial agreements) relating to the sharing of personal information.

Inter-agency working groups

14.67 In its report, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency*, IPART considered how regulation in New South Wales, including privacy regulation, has the potential to impede information sharing. IPART concluded that the New South Wales Government should

> [c]onvene an inter-agency working group of senior officers (including representatives from Privacy NSW) to identify further opportunities where it would be appropriate (ie, where it would provide net benefits to the community) to share or streamline information among government agencies. This may require an initial stock-take or inventory of current government information requirements.[93]

14.68 In DP 72, the ALRC proposed that the Australian Government should convene an inter-agency working group of senior officers to identify circumstances where it would be appropriate to share or streamline the sharing of personal information among Australian Government agencies.[94]

Submissions and consultations

14.69 A number of stakeholders supported this proposal.[95] The Public Interest Advocacy Centre (PIAC) supported the proposal on the condition that the working group includes, or at a minimum consults with, consumer groups and privacy advocates.[96] The School of Public Health at the University of Sydney submitted that

---

93 Independent Pricing and Regulatory Tribunal of New South Wales, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency: Other Industries—Final Report* (2006), 228.

94 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 11–3.

95 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Federal Police, *Submission PR 545*, 24 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Confidential, *Submission PR 448*, 11 December 2007.

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

the OPC should work closely with the inter-agency working group and organisations that match or link information to ensure that all such activities occur to consistently high standards.[97]

14.70 Some stakeholders suggested there should be state and territory representation on the working group. For example, the Queensland Government submitted that it would seek representation if a working group on the sharing of information between federal, state and territory law enforcement or related agencies is convened.[98] Another stakeholder noted that a working group should include state government agencies, including licensing authorities, as these agencies are increasingly being used as identity verification agencies.[99]

14.71 Others opposed the proposal. The OPC submitted that the intent of the proposal is unclear and that the working group does not provide the necessary specific and reasoned consideration of privacy obligations.

> In the view of the Office, any proposal for sharing information between agencies should be considered and assessed on its own merits by the respective agencies involved, with a view to the necessary legislative requirements and obligations governing the handling of the information. A Privacy Impact Assessment (PIA) of the proposed information sharing project would be a crucial, underpinning element of these considerations. Agencies are encouraged to consult with the Office in regard to privacy risks identified in a PIA.[100]

14.72 The Australian Privacy Foundation submitted that it should not be a function of a privacy law to search out data-sharing opportunities—the immediate need is for a standing body to review any such proposals, whatever their origin, in light of privacy obligations.[101]

ALRC's view

14.73 Submissions and consultations with stakeholders suggested that regular discussion through an inter-agency working group facilitated information sharing while still accommodating privacy requirements.

14.74 The ALRC notes that it may be useful to convene interjurisdictional inter-agency working groups when the Australian Government wants to share personal information with state and territory government agencies. This will be the case particularly where Australian Government and state and territory government agencies are subject to different legislative requirements, including privacy requirements—

---

97 School of Public Health—University of Sydney, *Submission PR 504*, 20 December 2007.
98 Queensland Government, *Submission PR 490*, 19 December 2007.
99 P Youngman, *Submission PR 394*, 7 December 2007.
100 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
101 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

although the ALRC's recommendation for the application of the UPPs across the federal, state and territory public sectors and the private sector should minimise the circumstances in which this issue may arise.

14.75 As noted above, the ALRC encourages information-sharing opportunities that are in the public interest and lessen compliance burdens on agencies, businesses and the community. The ALRC is not of the view, however, that the Australian Government should convene an inter-agency working group of senior officers to identify circumstances where it would be appropriate to share or streamline personal information.

14.76 In the ALRC's view, it is not appropriate or necessary to convene such a working group. The ALRC agrees with the OPC that any proposal for sharing information between agencies should be considered and assessed on its own merits with a view to the necessary legislative requirements and obligations governing the handling of the information.

Information sharing by law enforcement and intelligence agencies

14.77 Government agencies across the world increasingly are searching for new ways to prevent and solve crime, particularly crimes associated with terrorism.[102] These new methods include new forms of intelligence gathering and the sharing of personal information, often across state, territory and national borders.[103]

14.78 The exchange of personal information among Australian Government agencies and state and territory government agencies for law enforcement purposes is, in most instances, regulated by privacy legislation or administrative schemes.[104] There is, however, a number of exemptions and exceptions that apply to law enforcement and intelligence agencies.

14.79 The Information Privacy Principles (IPPs) do not apply to the acts and practices of certain Australian Government law enforcement and intelligence agencies such as the Australian Crime Commission (ACC), the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS).[105] While some of these agencies are regulated by statutory guidelines that address the handling of personal information, the guidelines do not address interjurisdictional information

---

102 See J Lye and T McNeilly, 'Current Privacy Issues in National Security' (Paper presented at Australian Institute of Administrative Law 2006 National Administrative Law Forum, Surfers Paradise, 22–23 June 2006); A Cockfield, 'Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies' (2007) 40(1) *University of British Columbia Law Review* 41.

103 See, eg, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth); *Anti-Terrorism Act (No 2) 2005* (Cth); *Aviation Transport Security Act 2004* (Cth). See discussion of cross-border data flows in Ch 31.

104 See discussion of state and territory privacy regimes in Ch 2.

105 See discussion in Ch 37.

sharing (the sharing of information among federal, state and territory law enforcement and intelligence agencies).[106]

14.80 Section 7 of the *Privacy Act* exempts the acts and practices of agencies from the operation of privacy principles, if the act or practice relates to personal information that has originated with, or has been received from, specified law enforcement and intelligence agencies; or if the act or practice involves disclosure of personal information to ASIO, ASIS or the Defence Signals Directorate (DSD).

14.81 Law enforcement agencies that are not exempt from the operation of the *Privacy Act* often will be able to share personal information under one of the exceptions set out in the IPPs. These exceptions include where:

- the use or disclosure of personal information is required or authorised by or under law;
- the use or disclosure of personal information is reasonably necessary for the enforcement of the criminal law; or
- there is a reasonable belief that use or disclosure is necessary to prevent or lessen a serious and imminent threat to life or health.[107]

14.82 A law enforcement exception or exemption often is found in state and territory privacy legislation. For example, the *Privacy and Personal Information Protection Act 1998* (NSW) provides that a New South Wales government agency is not required to comply with certain privacy principles if the handling of personal information is reasonably necessary for law enforcement purposes.[108]

14.83 Codes and guidelines on the handling of personal information by law enforcement agencies have been developed by privacy regulators in some jurisdictions.[109] These documents do not, however, deal with interjurisdictional information sharing. Further, law enforcement agencies in some jurisdictions are not subject to any privacy regulation.[110]

---

106 These guidelines are discussed in Chs 34 and 37. These agencies also are subject to oversight by the Inspector-General of Intelligence and Security or the Australian Commission for Law Enforcement Integrity.

107 The ALRC makes a number of recommendations in relation to these exceptions in Part D.

108 *Privacy and Personal Information Protection Act 1998* (NSW) s 23. See also *Information Privacy Act 2000* (Vic) s 13.

109 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001); Office of the NSW Privacy Commissioner, *Privacy Code of Practice: Law Enforcement and Investigative Agency Access to Personal Information Contained in Public Registers*.

110 See discussion in Ch 2.

14.84 Should the Australian Government develop a framework for the sharing of personal information among Australian Government, and state and territory law enforcement and intelligence agencies? The United States Government has released *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (the Guidelines).[111] The Guidelines reflect 'basic privacy protections', requiring agencies to: identify, among other things, any privacy-protected information to be shared; assess and document applicable legal and policy rules and restrictions; put in place accountability and audit mechanisms, implement data quality and, where appropriate, redress procedures; and appoint a Privacy Official to ensure compliance with the Guidelines.[112]

14.85 In DP 72, the ALRC proposed that the Australian Government, in consultation with state and territory governments, intelligence agencies, law enforcement agencies, and various accountability bodies,[113] should:

- develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

- develop memorandums of understanding to ensure that accountability bodies can oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.[114]

---

111 United States Government Office of the Director of National Intelligence, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (2006). The 'Information Sharing Environment' has been described as 'the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of all federal executive branch entities to facilitate terrorism information sharing, access, and collaboration among users in order to combat terrorism more effectively': Program Manager—Information Sharing Environment, *Information Sharing Environment Privacy Guidelines—Frequently Asked Questions* (2006) United States Government Office of the Director of National Intelligence <www.ise.gov> at 7 May 2008. See also United States Government, *National Strategy for Information Sharing* (2007), 27.

112 Program Manager—Information Sharing Environment, *Information Sharing Environment Privacy Guidelines—Frequently Asked Questions* (2006) United States Government Office of the Director of National Intelligence <www.ise.gov> at 7 May 2008.

113 Including the OPC; the Inspector-General of Intelligence and Security; the Australian Commission for Law Enforcement Integrity; state and territory privacy commissioners and agencies with responsibility for privacy regulation; and federal, state and territory ombudsmen.

114 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 11–4.

Submissions and consultations

14.86 A number of stakeholders supported this proposal.[115] For example, the OPC submitted that the proposal would be a welcome addition to the public's understanding of what, when and how information is shared among law enforcement agencies and the accountability mechanisms that govern such activities. The OPC noted that in its submission to the 2007 Parliamentary Joint Committee on the ACC Inquiry into the future impact of serious and organised crime on Australian society,[116] it had suggested that:

> government agencies not subject to the statutory privacy regulation should develop and implement information handling practices that incorporate principles similar to those contained within the *Privacy Act*; and privacy guidelines could be included as part of any memorandum of understanding or agreement between jurisdictions.[117]

14.87 Privacy NSW submitted that Australians should be aware of the information-sharing arrangements in place among Australian intelligence and law enforcement agencies and their international counterparts.[118]

14.88 The AFP supported the proposal if there were appropriate exemptions for operationally sensitive matters—for example, police or intelligence methodology.[119]

14.89 The Australian Government Department of Agriculture, Fisheries and Forestry submitted that the Australian Quarantine and Inspection Service should be included in developing this framework because it has similar interests to those of a law enforcement agency.[120] The Australian Government Department of Human Services supported the proposal. It noted that assistance regarding proof of identity documentation could be provided by other agencies, including those within the Human Services portfolio.[121]

---

115 Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Law Council of Australia, *Submission PR 527*, 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; Privacy NSW, *Submission PR 468*, 14 December 2007.

116 See Australian Parliament—Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into the Future Impact of Serious and Organised Crime on Australian Society* (2007) <www.aph.gov.au> at 6 February 2008.

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

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

119 Australian Federal Police, *Submission PR 545*, 24 December 2007.

120 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

121 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

14.90 Some stakeholders supported the proposal, but submitted that the framework should:

- facilitate information sharing with private sector organisations such as airlines and airports with important security responsibilities;[122]
- consider the interaction between the law enforcement and intelligence agencies and other agencies that routinely become involved in such processes, such as birth, deaths and marriages, Centrelink and licensing authorities;[123] and
- include an effective mechanism to ensure consumer input into any consultative process.[124]

14.91 Other stakeholders opposed the proposal. One stakeholder argued that law enforcement agencies already have a framework of information sharing or intelligence exchange.[125] Foreign Intelligence Agencies of the Australian Intelligence Community submitted that the ALRC should provide a clearer rationale for the proposal. The Agencies submitted that it is not clear, for example, how existing arrangements might be defective, or might have led to unreasonable intrusions into the privacy of Australians.[126]

ALRC's view

14.92 The ALRC acknowledges that the broader social interest in national security and law enforcement issues often will override privacy interests. The ALRC is concerned, however, that agencies with responsibility for national security and law enforcement often are exempt from privacy legislation. Further, not all exempt law enforcement and intelligence agencies are subject to statutory guidelines or other rules that govern the sharing of personal information. The ALRC also has found that these rules are not always publicly accessible.

14.93 In the absence of comprehensive rules to deal with the sharing of personal information among federal, state and territory law enforcement and intelligence agencies, the Australian Government should develop a framework relating to interjurisdictional sharing of personal information within Australia by such agencies. In the interest of transparency, this framework should be made available to the public.

14.94 While national security and law enforcement are important, implementation of measures to protect Australian citizens often results in an invasion of an indidviaul's privacy. The development and publication of a framework relating to interjurisdictional

---

122 Confidential, *Submission PR 536,* 21 December 2007.
123 P Youngman, *Submission PR 394,* 7 December 2007.
124 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.
125 Confidential, *Submission PR 448,* 11 December 2007.
126 Foreign Intelligence Agencies of the Australian Intelligence Community, *Submission PR 466,* 13 December 2007.

sharing and the development of memorandums of understanding between accountability bodies will help to ensure an appropriate balance between national security, law enforcement and an individual's right to privacy.

14.95 The framework should be developed in consultation with relevant bodies including state and territory governments, intelligence agencies, law enforcement agencies, and various accountability bodies. These accountability bodies include: the OPC, state and territory privacy commissioners and agencies with responsibility for privacy regulation; bodies with responsibility for overseeing law enforcement and intelligence agencies, including the Australian Commission for Law Enforcement Integrity and the Inspector-General of Intelligence and Security; and federal, state and territory ombudsmen.

14.96 The ALRC does not recommend the development of memorandums of understanding to ensure that accountability bodies can oversee interjurisdictional information sharing within Australia. The ALRC was concerned that this proposal suggested that the oversight powers of some accountability bodies should be extended to cover the acts and practices of law enforcement and intelligence agencies that are not currently within their jurisdiction.

14.97 Instead, the ALRC recommends the development of memorandums of understanding to clarify the existing roles of accountability bodies that oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies. This oversight would include reporting and the auditing of law enforcement and intelligence agencies.

Recommendation 14–2 The Australian Government, in consultation with: state and territory governments; intelligence agencies; law enforcement agencies; and accountability bodies, including the Office of the Privacy Commissioner, the Inspector-General of Intelligence and Security, the Australian Commission for Law Enforcement Integrity, state and territory privacy commissioners and agencies with responsibility for privacy regulation, and federal, state and territory ombudsmen, should:

(a) develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

(b) develop memorandums of understanding to clarify the existing roles of accountability bodies that oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.

Government contractors

14.98 While information about federal, state and territory privacy regimes is publicly available, Australian Government, and state and territory agency contracts are not. This makes it difficult to detect whether contractual privacy provisions are inconsistent with the *Privacy Act*.[127]

14.99 The OPC has expressed the view that, in many cases, contractual privacy provisions are an appropriate way to incorporate higher privacy obligations than may otherwise apply, or to maintain privacy protections that apply already to personal information. For example, they may compel a contractor to undertake specific privacy-related activities, such as mandatory reporting of suspected privacy breaches, or to undertake staff training.[128]

14.100 Other stakeholders expressed the view that privacy clauses in contracts often are overly legalistic, claiming to cover all possibilities but too often failing to allocate clearly responsibility for breaches.[129] It was suggested that Australian agencies have taken an inconsistent approach to documents containing information regulated by the *Privacy Act*.[130]

Commonwealth contracts

14.101 The *Privacy Act* imposes obligations on agencies entering into contracts to provide services to or on behalf of the agency. Section 95B requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract, or a subcontractor, does not do an act or engage in a practice that would breach the IPPs. The Act defines a 'contracted service provider' as 'an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract', or a subcontractor for the government contract.[131]

14.102 A small business that is also a contracted service provider will be subject to the *Privacy Act* in respect of the performance of that contract.[132] A state or territory authority contracting with an agency will not be covered by the Act. A 'State contract' is defined as a 'contract, to which a state or territory or state or territory authority is or was a party, under which services are to be, or were to be, provided to a state or

---

127 The Australian Government Solicitor has drafted a model clause to assist agencies in discharging their responsibilities under the *Privacy Act 1988* (Cth): Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 7–8.

128 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

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

130 National Association for Information Destruction, *Submission PR 133*, 19 January 2007.

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

132 Ibid s 6D(4)(e).

territory authority'.[133] Section 16F of the Act provides that an organisation must not use or disclose personal information for direct marketing unless the use or disclosure is necessary to meet an obligation under the contract.

14.103 An act done or practice engaged in by a contracted service provider for the purposes of meeting an obligation under a contract will not breach an NPP or an approved privacy code if the act or practice is authorised by the contract. Therefore, the NPPs or a code can be varied by the contract and a breach of an NPP or code will not have occurred if the contractual obligations require the contracted service provider to do an act or practice that would be inconsistent with an NPP or an approved code to which it is bound.[134]

14.104 The Privacy Commissioner has jurisdiction to investigate the action of a contractor or subcontractor. Section 13A(1)(c) provides that a breach of a 'non-complying' privacy provision in a Commonwealth contract is an interference with privacy. The standards the Privacy Commissioner would apply in investigating a complaint are those set out in the contract.[135]

14.105 The obligations under s 95B extend to a contracted service provider who is not within Australia.[136] Although the Privacy Commissioner could take action overseas to investigate complaints, enforcement of the provisions of the contract overseas may be difficult.[137]

14.106 In DP 72, the ALRC did not make any proposals to amend the Commonwealth contractor provisions under the *Privacy Act*. The ALRC noted the OPC's submission that the Act does not restrict Australian Government agencies from including contractual clauses that refine existing privacy obligations, or impose additional obligations on a contractor, which may be appropriate under certain circumstances. The OPC submitted that, in this regard, the current provisions are appropriate and effective.[138] The OPC stated, however, that the definition of 'contracted service

---

133 The Australian Government Solicitor has advised, however, that notwithstanding this exclusion, agencies need to be mindful of the obligation under IPP 4(b) to ensure that everything reasonable is done to prevent unauthorised use or disclosure of personal information when contracting with a state or territory authority: Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 4.

134 *Privacy Act 1988* (Cth) ss 6A(2), 6B(2). See also Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 5.

135 Office of the Federal Privacy Commissioner, *Privacy Obligations for Commonwealth Contracts*, Information Sheet 14 (2001).

136 *Privacy Act 1988* (Cth) s 5B.

137 Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 4.

138 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.

provider' in the Act could be reviewed to ensure that it is adequate to cover all the types of activities that private sector organisations might perform on behalf of agencies.[139]

14.107 A number of stakeholders considered that the provisions are unclear and require redrafting.[140] For example, the OVPC submitted that it is not clear whether contracted service providers are able to contract out of their obligations under the NPPs or a code, and highlighted difficulties about the enforceability of provisions that purport to bind contractually a service provider to the privacy obligations of a government agency.[141]

14.108 The ALRC expressed the preliminary view that the contracted service provider provisions under the *Privacy Act* remain appropriate and effective. The ALRC, however, did ask whether the definitions of 'contracted service provider' and 'State contract' under the *Privacy Act* are adequate, and whether they covered all the types of activities that organisations might perform on behalf of agencies.[142]

Submissions and consultations

14.109 A number of stakeholders submitted that the definitions under the *Privacy Act* are adequate and cover all the types of activities that organisations might perform on behalf of a government agency.[143] Privacy NSW submitted, however, that the term and definition of 'contracted service provider' be replaced with a term and definition covering a broader spectrum of arrangements such as data services, temporary employees and students. It submitted that the definition should be as inclusive as possible, and suggested the following: 'a person employed or engaged by the agency or organisation in the course of employment or engagement'.[144]

14.110 Privacy NSW also submitted that, where agencies and organisations engage with third party entities, those third parties should be required to ensure that 'sub-contractors' are also bound to comply with the UPPs. Further, the agency or organisation should be responsible for the information while it is subject to dealings with a third party. This will enable individuals to know to whom to complain in the event that they believe that there has been an interference with their privacy.[145]

---

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

140 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

141 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

142 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 11–1.

143 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

145 Ibid.

14.111 National Legal Aid submitted that the current provisions create an arbitrary and somewhat artificial distinction between the way governments contract with organisations to provide government services and the way they fund organisations to provide services that benefit the community. In this sense, it argued, the provisions are confusing. It noted that the adoption of the ALRC's reforms for more uniform privacy legislation and for removing exemptions from the definition of organisations may remove some of the complexity.[146]

14.112 The OVPC reiterated its view that it is unclear whether contracted service providers are able to contract out of their obligations under the NPPs or a code. The OVPC suggested that the position in Victoria is clearer in this regard. In principle, organisations cannot contract out of their privacy obligations under the *Information Privacy Act 2000* (Vic).[147] The OVPC noted that this is not to say that the provisions under the *Information Privacy Act* are necessarily the best model.[148]

14.113 PIAC submitted that the provisions dealing with contracted service providers should be amended to make it clear that organisations cannot contract out of their privacy obligations and responsibilities. It submitted that provisions similar to the contractor provisions under the *Information Privacy Act* should be incorporated into the *Privacy Act*.[149]

14.114 The OVPC highlighted issues related to the enforceability of provisions that purport contractually to bind a service provider. It submitted that there are two options for dealing with this issue:

- make outsourcing or funding agencies responsible for the actions of their contractors and leave it to the government agencies to pursue the contractor for privacy breaches through indemnities; or

- leave the outsourcing agency and contracted service provider both liable for privacy breaches and allow the complainant the option of pursuing either or both—similar to the situation with manufacturer and retailer liability.

---

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

147 Although this was permitted during a phase-in period when the *Information Privacy Act 2000* (Vic) first came into force, contractors are now expected to ensure their contractual provisions are in accordance with their legislative obligations under privacy legislation and any other relevant laws: *Information Privacy Act 2000* (Vic) s 16(2) and (3).

148 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

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

14.115 In the OVPC's view, the first option provides greater clarity and suggests that accountability rests with the government. The second option gives the complainant greater flexibility to pursue parallel or alternative rights to seek redress.[150]

ALRC's view

14.116 The definitions of 'contracted service provider' and 'State contract' under the *Privacy Act* are adequate. The ALRC notes the comments by Privacy NSW that the definitions should be amended to include a broader range of arrangements such as data services, temporary employees and students. In the ALRC's view the current definitions would capture these arrangements. This definition also would capture Public Private Partnerships (PPPs) that are established by contract.[151]

14.117 The ALRC also has concluded that the *Privacy Act* provisions relating to Commonwealth contractors remain appropriate and effective. The ALRC notes the comments of stakeholders that the contracted service provider provisions are unclear. While the ALRC does not share this view, the redraft of the *Privacy Act* recommended in Chapter 5 may deal with these concerns.

14.118 Problems caused by government contractors being subject to two or more sets of privacy principles will be addressed partly by the UPPs replacing the IPPs and NPPs. The ALRC is conscious, however, that it still will be possible for a federal agency and an organisation to be subject to different privacy standards.

14.119 An agency may be subject to more stringent privacy standards than a contracted service provider. For example, under the 'Direct Marketing' principle an organisation is permitted to use or disclose personal information in certain circumstances for the purposes of direct marketing, an agency is not. Further, because of the operation of the different exceptions for organisations and agencies under the 'Access and Correction' principle, an organisation may be permitted to provide access to personal information in circumstances where an agency would not. This is because the 'Access' principle that relates to agencies is constrained by the limits of the *Freedom of Information Act 1982* (Cth). Conversely, an agency—such as a law enforcement or intelligence agency—may be exempt from complying with the *Privacy Act*, while an organisation may still be subject to all the UPPs.

14.120 The government contractor provisions of the *Privacy Act* provide an adequate solution to this problem. It is appropriate that organisations should be subject to the same privacy principles as an agency when contracting with that agency. The ALRC has therefore concluded that the provisions should be retained to ensure that

---

150 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

151 Public Private Partnerships are characterised by 'a long-term, whole-of-life commitment by the contractor to deliver and maintain new or redeveloped infrastructure used by a government agency to deliver services to the public': Australian Government Department of Finance and Administration, *Public Private Partnerships: Contract Management* (2006), 6.

organisations that contract with an Australian Government agency are subject to the same privacy principles as the agency itself.

14.121 The government contractor provisions could result in an organisation being subject to the more stringent privacy obligations of an agency. The ALRC acknowledges, however, that the government contractor provisions could result in an organisation having to comply with a contract provision that imposes less stringent privacy obligations on the organisation than it would usually be required to comply with under the UPPs. Section 95C of the *Privacy Act* provides some transparency in relation to these arrangements.[152] In the ALRC's view, this provision should be retained.

14.122 Other *Privacy Act* provisions relating to government contractors also should be retained, including those relating to direct marketing. If the ALRC's recommendation to remove the small business exemption is not implemented, the equivalent of s 6D of the *Privacy Act* should be retained. Section 6D provides that a small business that is also a contracted service provider is subject to the *Privacy Act* in respect of the performance of that contract.[153]

14.123 It is unnecessary to amend the *Privacy Act* to clarify whether the outsourcing agency or a contracted service provider is liable for an interference with privacy. Liability for the acts or practices of a contractor will depend on the facts of the case, including the terms of the contract. In the ALRC's view, the *Privacy Act* ensures that contracting out of government services does not result in a loss of accountability for the handling of personal information. As outlined above, the *Privacy Act* provides that organisations (including small businesses) that are government contractors are regulated under the Act, and that an outsourcing agency is required to take contractual measures to ensure that a government contractor complies with the privacy principles. Further, where the actions of a contractor results in an interference with privacy, individuals may make a complaint to the Privacy Commissioner.

National consistency issues

14.124 The privacy regimes in some states and territories include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs. Although the privacy principles in the various state and territory regimes often resemble the IPPs and NPPs, they are not identical.

---

152 The section provides that if a person asks a party to a Commonwealth contract to be informed of the content of provisions (if any) of the contract that are inconsistent with an approved privacy code binding a party to the contract or with an NPP, the party requested must inform the person in writing of that content (if any).

153 See Ch 39.

14.125 The OPC Review was told that contracted service providers can be required to comply with three sets of privacy principles—the NPPs which apply to them in their capacity as private sector organisations, the IPPs which apply to them under contracts granted in accordance with s 95B of the *Privacy Act*, and any applicable state or territory privacy laws.[154] This may be an issue particularly for organisations that provide contracted services involving personal information to federal, state or territory agencies.

14.126 Telstra advised the OPC Review that the proliferation of state legislation and inconsistency between state and federal legislation can add costs to conducting business with government agencies.[155] The OPC recommended that the Australian Government consider reviewing the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations. In its view, this would address the issues surrounding government contractors.[156]

14.127 National consistency issues were raised in a number of submissions to this Inquiry.[157] A number of stakeholders submitted that the development of a single set of principles that applied at the federal, state and territory level would deal with national consistency issues.[158] For example, Telstra noted that contractors to state governments are not bound by privacy rules in some states, and submitted that such issues could be resolved through the introduction of a single set of privacy principles across all Australian jurisdictions.[159]

14.128 The adoption of the UPPs, any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act* at the federal, state and territory level will deal with many of the national consistency issues that affect contracted government service providers.

---

154 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, 13.

155 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 37.

156 Ibid, 8 and rec 5. See Ch 18.

157 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; CSIRO, *Submission PR 176*, 6 February 2007; NSW Commission for Children and Young People, *Submission PR 120*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

158 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

159 Telstra, *Submission PR 185*, 9 February 2007. See also Law Council of Australia, *Submission PR 177*, 8 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

Contractor provisions under state and territory privacy regimes

14.129 Some state and territory privacy regimes require organisations that provide contracted services to a state or territory government agency to be bound by the relevant state privacy principles for the purposes of the contract.[160] Other state regimes provide that compliance with the state privacy regime is subject to any outsourcing arrangements,[161] or are silent on this issue.[162]

Submissions and consultations

14.130 The OPC submitted that it has ongoing concerns that state or territory government contractors, that are otherwise organisations, may not be bound by the *Privacy Act* or equivalent standards when performing functions under state or territory contracts. The OPC noted that the absence of consistent regulation for state contractors and the possible imposition of different obligations can create gaps in privacy protection and confusion about which body should regulate the privacy practices of state contractors.

> For example, in one instance, the Office had to decline to investigate a worker's compensation matter because it involved a state contractor, but no state privacy regime existed to deal with the matter. In other cases, both the Office and state privacy bodies have declined to investigate the practices of a state contractor.[163]

14.131 The OPC submitted that state and territory contractors should be covered by the *Privacy Act*, or equivalent legislation. The OPC noted that this could be achieved by all states and territories enacting privacy legislation which imposes obligations on their agencies and contractors that are at least equivalent to the *Privacy Act*. The OPC submitted in the alternative that the *Privacy Act* could be amended to ensure that the NPPs apply to state contractors where no equivalent state or territory privacy laws exist.[164]

14.132 The OVPC submitted that the current provisions for 'government contracts' and 'contracted service providers' in the *Privacy Act* do not align completely with provisions for 'state contracts' and 'contracted service providers' in the *Information Privacy Act*. The OVPC submitted that there are several issues that arise when contractors provide services to federal and state agencies, or operate in more than one jurisdiction. For example:

---

160 See, eg, *Information Privacy Act 2000* (Vic) s 17; *Information Act 2002* (NT) s 149.
161 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].
162 See, eg, *Privacy and Personal Information Protection Act 1998* (NSW); South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).
163 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
164 Ibid.

- cross-border data flow issues may arise where an organisation contracts with a recipient who is subject to a dissimilar privacy regime, or to no privacy regime at all;

- additional complexities arise in some cases, where organisations operating in more than one state or territory are bound by privacy schemes that pre-dated and may, in some cases, conflict or override Victorian privacy law;

- there is uncertainty about the employee records exemption continuing to apply where a state contract applies; and

- there have been problems in working out what a 'state contract' is, and whether the services are of a public kind. If an organisation falls under the exemption in the *Privacy Act* and is not picked up by the state Act (or the state has no privacy law in place), then the agency falls through the gap and its clients' information is not protected under any privacy law.[165]

14.133 The OVPC also submitted that the *Privacy Act* should be amended to recognise that state privacy laws may apply to contracted service providers seeking to be covered by a code under the *Privacy Act*, and to import a requirement to consult with and seek the approval of the states before any code covering state contracts is approved.[166]

ALRC's view

14.134 The Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that it was the intention of the Australian Parliament that the acts and practices of state and territory contractors would 'not be covered by the Commonwealth's privacy scheme but rather the State or Territory's own privacy standards'.[167]

14.135 Organisations that contract with a state government should be regulated by privacy legislation. The ALRC considered recommending that the *Privacy Act* be amended to include a 'roll-back provision' to cover state contractors. It is the ALRC's view, however, that such a law would intrude too heavily on state and territory government business. Instead, the ALRC recommends that state and territory privacy legislation should include provisions relating to state and territory contractors.[168] This is discussed in Chapter 3.

---

165 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
166 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.
167 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 8.
168 See Rec 3–4.

14.136 In the ALRC's view, organisations would rarely seek to be covered by a code under the *Privacy Act* in relation to state contracts. The ALRC does not agree that the *Privacy Act* should be amended to include a requirement for the OPC to consult with and seek the approval of the states before any code is approved covering state contracts. This requirement will not be necessary if each state and territory introduces provisions to regulate government contractors in that jurisdiction. As discussed in Chapters 3 and 17, this issue could be addressed in a memorandum of understanding between the OPC and state and territory privacy regulators. This memorandum of understanding could also set out a process for developing and publishing joint guidance on government contracted service providers for agencies and organisations.

14.137 The ALRC notes that many of the issues identified by the OVPC in its submission are dealt with in other chapters of this Report. Issues related to cross-border data flows are dealt with in Chapter 31 and the employee records exemption is considered in Chapter 40.

15. Federal Information Laws

Contents

Introduction

15.1 This chapter considers how the *Privacy Act 1988* (Cth) interacts with a number of federal laws that regulate the handling of personal information. The chapter first discusses the interaction between the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) (FOI Act) and the *Archives Act 1983* (Cth), and considers whether the three Acts should be combined in the one Act and administered by a single body. The chapter then examines how the *Privacy Act* interacts with secrecy provisions in federal legislation. The final section of the chapter considers whether the confidentiality provisions in Part VIII of the *Privacy Act* are still required.

Freedom of Information Act 1982 (Cth)

15.2 The interrelationship between the FOI Act and the *Privacy Act* is significant. Both Acts regulate the way in which information is handled in government, but have

different objectives. Freedom of information legislation is concerned mainly with transparency in government and protects privacy only to the extent that it prevents the unreasonable disclosure of personal information, and provides for the access and correction of personal information. In contrast, privacy legislation is primarily focused on data protection and provides for transparency only to the extent that it enhances the information privacy rights of individuals.[1] The *Privacy Act* is designed to interact with the FOI Act. For example, the public sector exemptions under the *Privacy Act* largely mirror the exemptions under the FOI Act.[2]

Disclosure of personal information

15.3 The FOI Act provides that every person has a legally enforceable right to obtain access to a document of an agency or an official document of a minister, other than an exempt document.[3]

15.4 Section 41(1) of the FOI Act provides that a document is an exempt document if its disclosure under the Act would involve the unreasonable disclosure of personal information about any person (including a deceased person). The definition of 'personal information' in the FOI Act corresponds with that in the *Privacy Act*.[4] The exemption under s 41(1) is subject to an exception that a person cannot be denied access to a document on the basis that it contains his or her own information.[5] It does not prevent reliance on the exemption, however, where the information cannot be separated from personal information about another person.[6] The exemption under s 41 has been the subject of criticism and commentary.[7]

15.5 In *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), the ALRC and the Administrative Review Council (ARC) concluded that the provision should be amended to clarify the relationship between the FOI Act and the *Privacy Act*. To this end, the review concluded that s 41 should be reworded to provide that a document is exempt if it contains personal information, the disclosure of which would constitute a breach of Information Privacy Principle (IPP) 11; and the disclosure would not, on balance, be in the public interest.[8] The review also

---

1 See M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [1.47]. The ALRC considered these issues in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).

2 See discussion in Ch 36.

3 *Freedom of Information Act 1982* (Cth) s 11.

4 Ibid s 4. See Ch 6 for discussion of the definition of 'personal information' under the *Privacy Act*.

5 Ibid s 41(2).

6 See, eg, *Re Forrest and Department of Social Security* (1991) 23 ALD 131; M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [6.25].

7 See Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 10; Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001).

8 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [10.7] and Rec 59.

recommended that a Freedom of Information Commissioner[9] should issue guidelines to assist agencies to determine whether information is exempt under s 41.[10] These recommendations have not been implemented.[11]

15.6 In the Discussion Paper, *Review of Privacy* (DP 72), the ALRC expressed the preliminary view that s 41 of the FOI Act should be amended to clarify the relationship between the FOI Act and the *Privacy Act*. The ALRC proposed that s 41(1) of FOI Act be amended to provide that a document is exempt if it:

- contains personal information, and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle and disclosure would not, on balance, be in the public interest; or
- contains personal information of a deceased individual, and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle and disclosure would not, on balance, be in the public interest. Where the 'Use and Disclosure' principle would require consent the agency must consider whether the proposed disclosure would involve the unreasonable disclosure of personal information about any individual including the deceased individual.[12]

15.7 The ALRC also proposed that the definition of 'personal information' in the FOI Act should be aligned with the ALRC's proposed definition in the *Privacy Act* as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual';[13] and that the FOI Act should be amended to require the body that is primarily responsible for administration of that Act to develop and publish guidelines on the interpretation and application of s 41 in consultations with the Office of the Privacy Commissioner (OPC).[14]

---

9 Ibid, [6.4] and Rec 18. See the discussion of a Freedom of Information Commissioner below.

10 Ibid, [10.8] and Rec 60.

11 See, however, the Freedom of Information Amendment (Open Government) Bill 2000 (Cth); Freedom of Information Amendment (Open Government) Bill 2003 [2004] (Cth); and Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001).

12 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–2. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [6.24]. The Senate Legal and Constitutional Legislation Committee supported a similar amendment in Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.52].

13 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–3.

14 Ibid, Proposal 12–4.

Submissions and consultations

15.8 A number of stakeholders supported the proposal to amend s 41 to clarify the relationship between the FOI Act and the *Privacy Act*.[15] Other stakeholders, however, raised a number of concerns about the proposed reform.[16] For example, the Australian Government Department of Foreign Affairs and Trade (DFAT) submitted that the proposed reform would be problematic to the extent that it required DFAT to obtain the consent of an individual before disclosing his or her personal information. In circumstances where a document contained joint personal information the proposal would, in effect, enable one person to veto the release of a document to another person. Further, the proposed reform would increase the time required to process FOI requests, particularly given the fact that documents held by DFAT often contained personal information about DFAT employees.[17]

15.9 Some stakeholders supported the ALRC's proposal to amend the definition of 'personal information' in the FOI Act.[18] Others raised various issues with the proposal.[19] For example, the Public Interest Advocacy Centre (PIAC) did not support the inclusion of 'an opinion' in the definition of 'personal information' because it has the potential to make the definition too wide.[20] A number of stakeholders supported the proposal for the development and publication of guidelines on the interpretation and application of s 41.[21]

ALRC's view

15.10 On 24 September 2007, following the release of DP 72, the then Attorney-General of Australia requested that the ALRC examine and report on the extent to

---

15 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 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.

16 Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008; Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Right to Know Coalition, *Submission PR 542*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

18 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; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

19 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008 referring to Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

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

21 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.

which the FOI Act and related laws continue to provide an effective framework for access to information in Australia.[22]

15.11 The ALRC acknowledges that a number of stakeholders addressed proposals to clarify the relationship between s 41 of the FOI Act and the *Privacy Act*. It is the ALRC's view, however, that these issues should be considered as part of the ALRC's review of the FOI Act. Section 41 primarily relates to access to personal information about third parties and not an individual's access to his or her personal information. It is therefore more appropriate for this issue to be considered in the context of the FOI Act. The ALRC therefore makes no recommendations in relation to s 41 in this Report.

Required or authorised by or under law

15.12 The current IPP 11 and the recommended 'Use and Disclosure' principle impose a general obligation on agencies not to disclose personal information to persons or organisations other than the individual concerned or his or her agent, unless one of the stated exceptions apply. A release of personal information under the FOI Act is unlikely to breach IPP 11 or the recommended 'Use and Disclosure' principle, as it would be 'authorised' by or under law.[23] As noted in *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), however, the meaning of 'authorised' in this context is not clear.

> On one view, any release of information pursuant to a request made under the FOI Act is an 'authorised' release of information. On another view, the FOI Act does not 'authorise' the release of information because s 14 of the Act makes it quite clear that nothing in the Act prevents the release quite apart from the Act of information that can be properly released.[24]

15.13 In ALRC 77, the ALRC and the ARC recommended that the *Privacy Act* be clarified to provide that a release of personal information under the FOI Act constitutes a release that is 'required or authorised by law' for the purpose of IPP 11.1(d).[25] This recommendation has not yet been implemented.

15.14 In DP 72, the ALRC expressed the view that, in the interest of certainty, this issue should be clarified in the FOI Act. The ALRC proposed that the FOI Act be amended to provide that disclosure of personal information in accordance with the FOI

---

22 The Terms of Reference are available on the ALRC website at <www.alrc.gov.au/inquiries /current/foi/terms.htm>.

23 *Privacy Act 1988* (Cth) s 14, IPP 11.1(d). Australian Government Attorney-General's Department, *Freedom of Information Memorandum 93: FOI and the Privacy Act* (1992) states that disclosure required under the FOI Act comes within this exception. See Ch 13 for discussion of federal laws that require or authorise disclosure of personal information.

24 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [10.23].

25 Ibid, [10.23]–[10.24] and Rec 65.

Act is a disclosure that is required or authorised by or under law for the purposes of the 'Use and Disclosure' principle.[26]

Submissions and consultations

15.15 A number of stakeholders supported the ALRC's proposal in DP 72.[27] Other stakeholders questioned the utility of the proposal. For example, the Australian Communications and Media Authority questioned whether such an amendment was required as there is 'no doubt' that disclosure under the FOI Act would be authorised by or under law for the purposes of the *Privacy Act*.[28]

15.16 The OPC supported the proposal but noted that it referred to a disclosure that was 'required or authorised' under the proposed 'Use and Disclosure' principle. The OPC submitted that it supports the adoption of a 'required or *specifically* authorised' test in the 'Use and Disclosure' principle.[29]

ALRC's view

15.17 In the interest of certainty, the FOI Act should be amended to provide that disclosure of personal information in accordance with the FOI Act is a disclosure that is required or authorised by or under law for the purposes of the 'Use and Disclosure' principle under the *Privacy Act*. The ALRC considered whether this issue should be dealt with in the ALRC's review of the FOI Act and related laws, but concluded that it directly affected the operation of the *Privacy Act* and should be considered as part of this Inquiry. To eliminate any possible confusion about the meaning of the exception so far as it relates to a release of information under the FOI Act, this issue should also be addressed in guidance issued by the OPC on the 'Use and Disclosure' principle.

Recommendation 15–1 The *Freedom of Information Act 1982* (Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act* is a disclosure that is required or authorised by or under law for the purposes of the 'Use and Disclosure' principle under the *Privacy Act*.

---

26 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–5. The ALRC noted that the requirement that the disclosure of personal information be 'in accordance with the FOI Act' would include that the consultation requirements under s 27A of the FOI Act had been satisfied.

27 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.

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

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

An exemption for the functions of the Privacy Commissioner?

15.18 In its submission to this Inquiry, the OPC raised the issue of whether its complaint files should be exempt from disclosure under the FOI Act. The OPC submitted that such complaints deal with the issue of privacy itself. It also noted that the Office of the NSW Privacy Commissioner's complaint-handling, investigative and reporting functions are exempt under the *Freedom of Information Act 1989* (NSW).[30]

15.19 The OPC noted that it is currently possible under the FOI Act to exempt, on a case-by-case basis, documents that may unreasonably disclose personal information.[31] The OPC submitted, however, that a 'cover-all' exemption would be consistent with public expectations of privacy, heighten the trust of complainants, and reinforce the OPC's commitment to leadership in good privacy practice.[32]

15.20 In DP 72, the ALRC asked whether the OPC's complaint-handling, investigative and reporting functions should be exempt under the FOI Act.[33]

Submissions and consultations

15.21 Privacy NSW submitted that any information relating to OPC complaint and 'own motion' investigation files should be exempt from access under FOI law because the subject of privacy complaints and investigation relates to personal information. Accordingly, disclosure to third parties could, in itself, give rise to complaints about interferences with privacy.[34] Other stakeholders did not support an exemption in relation to the OPC's complaint-handling, investigative and reporting functions. For example, PIAC submitted that such a provision could undermine public confidence in the transparency and accountability of the OPC.[35]

ALRC's view

15.22 The ALRC does not recommend in this Inquiry that the OPC's complaint-handling, investigative and reporting functions be exempt under the FOI Act. As noted above, 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.[36] Consideration of an exemption under the FOI Act for the OPC's complaint-handling, investigative and reporting functions would be more appropriately considered as part of that review.

---

30 See, eg, *Freedom of Information Act 1989* (NSW) s 9 and sch 2.

31 *Freedom of Information Act 1982* (Cth) s 41(1).

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

33 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 12–2.

34 Privacy NSW, *Submission PR 468*, 14 December 2007. See also P Youngman, *Submission PR 394*, 7 December 2007.

35 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

36 The Terms of Reference are available on the ALRC website at <www.alrc.gov.au/inquiries/current/foi/terms.htm>.

Access, correction and annotation

15.23 Both the FOI Act and the *Privacy Act* enable individuals to obtain access to, correct and annotate their own personal information held by agencies. The ALRC notes that different terminology is used in the *Privacy Act* and the FOI Act with respect to the correction of personal information.[37] In the interest of consistency with the 'Access and Correction' principle outlined in Chapter 29, this section of the chapter refers to 'correction' of personal information.

Privacy Act provisions

15.24 The rights to obtain access to, correct and annotate personal information provided by the *Privacy Act* are found in IPP 6 and IPP 7. The OPC has stated that as a result of the terms of IPPs 6 and 7, read in conjunction with other provisions of the *Privacy Act*,[38] it will generally decline to investigate a complaint about access to, or correction of, personal information held by an agency if the individual has not exhausted all FOI Act processes.[39] The OPC noted that this can result in complainant dissatisfaction and confusion, and unnecessary administrative costs and processes. Since 2001, the OPC has declined 17 complaints about access and seven complaints about correction.[40]

Access

15.25 IPP 6 provides that an individual will be entitled to have access to a record containing his or her personal information, except to the extent that the agency is required or authorised to refuse access to the record under any law of the Commonwealth that provides for access by persons to documents. The effect of this provision is to subject the right of access to personal information under the *Privacy Act* to the exemptions under the FOI Act. Section 34 of the *Privacy Act* prohibits the Privacy Commissioner from providing certain information about documents if they would be exempt under the FOI Act.

---

37 The heading in IPP 7 refers to 'alteration'; Part V of the FOI Act refers to 'amendment' of personal information. NPP 6 and the recommended 'Access and Correction' principle, however, refer to 'correction' rather than 'amendment'.

38 *Privacy Act 1988* (Cth) s 34.

39 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; *S v Various Commonwealth Agencies* [2004] PrivCmrA 8; 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. Section 41(1) of the *Privacy Act* provides that the Privacy Commissioner may decide not to investigate or not to investigate further a complaint if it is satisfied that the act or practice is the subject of an application under another Commonwealth enactment and the complaint has been or is being dealt with adequately under that enactment; or another Commonwealth enactment provides for a more appropriate remedy.

40 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. The OPC has declined these complaints under s 41(1)(f) of the *Privacy Act* on the grounds that the complaint would best be dealt with under another law.

Correction

15.26 Under IPP 7.1, an applicant may apply for correction of personal information on the grounds that it is inaccurate or, given its purpose, irrelevant, misleading, incomplete or not up-to-date. The FOI Act does not include a reference to 'purpose'.[41] IPP 7.1 provides for the correction of personal information in a wider range of circumstances than the FOI Act. An application for correction will need to be dealt with under the *Privacy Act* rather than the FOI Act where a person seeks:

- correction on the grounds that the information is irrelevant;
- deletion of personal information; or
- correction of personal information in a record to which he or she has not been provided lawful access.[42]

15.27 IPP 7.2 provides that the obligation imposed on an agency to correct personal information in IPP 7.1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents. The effect of IPP 7.2 is that the right to correction under IPP 7.1 will be subject to the requirements for an application for correction under Part V of the FOI Act.[43] These requirements are discussed in detail below.

Annotation

15.28 IPP 7.3 provides for the annotation of records containing personal information when:

- an agency is unwilling to correct a record containing an individual's personal information in accordance with a request by the individual; and
- no decision has been made to correct that information under an applicable provision of a law of the Commonwealth.

15.29 The limitation in IPP 7.3 is reflected in s 35 of the *Privacy Act*, which provides when the Privacy Commissioner may annotate personal information following an unsuccessful application under the FOI Act. Under s 35, the Commissioner's power to

---

41 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.17].

42 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), 18. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.23]–[4.24].

43 *Freedom of Information Act 1982* (Cth) ss 48–50. 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), 18. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.23]–[4.24].

direct an agency to annotate personal information is subject to a number of limitations including that:

- an application for review of a decision under the FOI Act has been finally determined or otherwise disposed of;
- the period within which an appeal may be made to the Federal Court has expired or, if such an appeal has been instituted, the appeal has been determined; and
- the effect of the review and any appeal is that access to the document is not to be given.

15.30 Section 35 of the *Privacy Act* ensures that even if a person cannot gain access to a document concerning them under the FOI Act and cannot succeed in getting the agency to amend the document, the Privacy Commissioner can still require the agency to annotate the document setting out the amendment that the Privacy Commissioner thinks appropriate. The OPC has noted that this practice is rarely used and that requests for correction which have the Privacy Commissioner's support are usually resolved without resort to the process.[44]

FOI Act provisions

Access

15.31 The FOI Act provides that every person has a legally enforceable right to obtain access to a document of an agency or an official document of a minister, subject to a number of exemptions under the Act.[45]

15.32 The majority of applications for access under the FOI Act relate to access to personal information. The *Freedom of Information Annual Report* states that in 2006–07, 87% of the 38,787 FOI requests received were for documents containing personal information. It is not clear from the report what percentage of these requests were from individuals seeking access to their own personal information. The remaining 13% of FOI requests were for documents concerning policy development and government decision making.[46]

Correction and annotation

15.33 The correction and annotation rights in the FOI Act are located in Part V[47] and were included in the FOI Act before the introduction of the *Privacy Act*. In 1987, the Senate Standing Committee on Legal and Constitutional Affairs recommended that the correction and annotation provisions be transferred from the FOI Act to privacy

---

44 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.

45 *Freedom of Information Act 1982* (Cth) s 11.

46 A request for personal information means a request for documents which contain information about a person: Australian Government Attorney-General's Department, *Freedom of Information Annual Report 2006–2007* (2007), [1.9]–[1.31].

47 *Freedom of Information Act 1982* (Cth) s 48.

legislation, 'should the latter be enacted'.[48] This did not happen when the *Privacy Act* was enacted in 1988. The *Freedom of Information Annual Report* notes that 1,379 FOI requests related to the correction of personal information in 2006–07.[49]

15.34 Part V sets out that an application for correction or annotation of personal information must satisfy a number of requirements, including:

- an individual must have been lawfully provided with the document under the FOI Act or otherwise;
- the document must have been used, be being used or be available for use, for an 'administrative purpose'; and
- the individual must apply in writing, the application must specify certain matters, and the application must be sent by post or hand delivered and specify a return address. [50]

15.35 The Part also provides that, to the extent that it is practicable, an agency must amend the document in a way that does not obliterate the text as it stood before the amendment.[51] Section 51 of the FOI Act provides that where an agency or minister decides not to amend a document or official documents under the Act, the agency or minister must take such steps as are reasonable in the circumstance to enable the applicant to provide a statement and annotate the document or official document with that statement.

Addressing the overlap

15.36 The access, correction and annotation provisions raise issues related to the overlap of the *Privacy Act* and the FOI Act and how the two Acts interact with each other. This section of the Chapter deals with the overlap of the two Acts. The interaction between the Acts is discussed later in the Chapter.

15.37 In ALRC 77, the ALRC and the ARC considered the overlap of the *Privacy Act* and FOI Act provisions relating to access to, and correction and annotation of, personal information, and concluded that it did not give rise to any major difficulties.[52]

---

48 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Freedom of Information Act 1982—The Operation and Administration of the Freedom of Information Legislation* (1987), [15.7].

49 Australian Government Attorney-General's Department, *Freedom of Information Annual Report 2006–2007* (2007), [1.9]–[1.32].

50 *Freedom of Information Act 1982* (Cth) ss 48–50.

51 Ibid s 50(3).

52 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [5.17].

Submissions to this Inquiry have noted, however, that the overlap can lead to confusion for agencies and the public.[53]

15.38 In DP 72, the ALRC expressed the preliminary view that an individual's right to obtain access to, or correct of, his or her own personal information held by an agency should be dealt with under a new Part in the *Privacy Act*. The ALRC proposed that:

- the *Privacy Act* be amended to include a new Part dealing with access to, and correction of, personal information held by an agency;
- the FOI Act be amended to provide that an individual's right to obtain access to, or correction of, his or her own personal information is dealt with under the *Privacy Act*; and
- Part V of the FOI Act be repealed.[54]

Submissions and consultations

15.39 A number of stakeholders supported these proposals.[55] Others submitted, however, that access to, and correction of, personal information held by agencies should be regulated by the 'Access and Correction' principle. It was submitted that having separate access and correction provisions for agencies and organisations in the *Privacy Act* would create confusion;[56] contradict the aim of creating a single set of privacy principles;[57] and would not address the problems caused by requests for access to documents containing personal and non-personal information,[58] or a mix of personal information about two or more individuals.[59] It was also noted that it is important that rules relating to health records were the same for the public and private sectors.[60]

15.40 Privacy NSW submitted that the proposed 'Access and Correction' principle should be divided into two sections, the first relating to organisations and the second to

---

53 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; Insurance Council of Australia, *Submission PR 110*, 15 January 2007; D Hall, *Submission PR 61*, 27 November 2006.

54 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 12–6 and 12–7.

55 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Confidential, *Submission PR 536*, 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; Australia Post, *Submission PR 445*, 10 December 2007.

56 Confidential, *Submission PR 570*, 13 February 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

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

58 See, eg, Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; National Legal Aid, *Submission PR 521*, 21 December 2007.

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

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

agencies.[61] The Social Security Appeals Tribunal (SSAT) suggested that the individual's 'right' to correction, or the agency's 'obligation' to correct, be set out in the *Privacy Act* and that the process provisions be retained in the FOI Act.[62]

15.41 Some stakeholders argued against the repeal of Part V of the FOI Act. Centrelink and the SSAT preferred the current arrangements where access and correction are dealt with under the FOI Act, noting that the FOI Act is already adequately structured to accommodate the access and correction process.[63] The OPC submitted that it would be more appropriate to expand the correction rights under the FOI Act to be consistent with those in the *Privacy Act*.[64]

15.42 National Legal Aid submitted that the proposal has implications in relation to national consistency of privacy laws relating to the federal and state and territory public sectors. It noted that some state privacy laws are subordinated to freedom of information laws and access to personal information is subject to FOI exemptions.[65]

Options for reform

15.43 In the ALRC's view, individuals should have access to a simple and user-friendly process to obtain access to, and correction of, their own personal information. The ALRC has considered various models for dealing with the overlap between the FOI Act and the *Privacy Act* in relation to access to, and correction of, personal information, including those contained in legislation in the United Kingdom, New Zealand and Canada.[66]

15.44 As outlined above, in DP 72, the ALRC proposed that the *Privacy Act* and the FOI Act be amended to provide that access to, and correction of, personal information be covered solely under a new Part in the *Privacy Act*. The ALRC modelled this proposal on the arrangements under the *Privacy Act 1993* (NZ) and the *Official Information Act 1982* (NZ).

15.45 One alternative is that access to, and correction of, personal information could be dealt with exclusively under the FOI Act. The ALRC is conscious, however, that the access procedures under the FOI Act can be cumbersome.[67]

---

61 Privacy NSW, *Submission PR 468*, 14 December 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

62 Social Security Appeals Tribunal, *Submission PR 478*, 17 December 2007.

63 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Social Security Appeals Tribunal, *Submission PR 478*, 17 December 2007.

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

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

66 Including the *Data Protection Act 1998* (UK); *Official Information Act 1982* (NZ); *Privacy Act 1993* (NZ); *Privacy Act 1985* (Canada); *Access to Information Act 1985* (Canada); *Freedom of Information and Protection of Privacy Act 1990* (Ontario); *Freedom of Information and Protection of Privacy Act 1996* (British Columbia).

67 The Attorney-General's Department recently reported that 67% of requests for correction of personal records took over 60 days to process: Australian Government Attorney-General's Department, *Freedom of Information Annual Report 2006–2007* (2007), [1.32].

15.46 Another alternative would be for access to personal information to be covered by the FOI Act, and correction of personal information to be covered by the *Privacy Act*. In the ALRC's view, however, it would be confusing for agencies and the public to have access to, and correction of, personal information covered by more than one Act.

15.47 A further option is to maintain the status quo. The ALRC notes, however, submissions from stakeholders that the current arrangements create confusion for agencies and the public. Another option is to maintain the current arrangements, but to modify the interaction between the access and correction provisions under the *Privacy Act* and the FOI Act. This option is discussed further below.

ALRC's view

15.48 The right to access and correct personal information held by an agency should not be dealt with solely under the *Privacy Act*. The existing arrangements whereby individuals have rights to obtain access to, and correction of, personal information under both the *Privacy Act* and the FOI Act should remain. In the ALRC's view, however, the provisions that deal with the interaction between the access and correction provisions under both Acts should be modified. This issue is discussed further below.

15.49 An agency's obligation to provide access to, and to correct, an individual's own personal information should not be dealt with under a separate Part of the *Privacy Act*. The ALRC agrees with stakeholders that such a proposal contradicts the aim of creating a single set of privacy principles to cover both agencies and organisations and could create confusion for agencies.

15.50 Instead the 'Access and Correction' principle should set out the requirements applicable to agencies in respect of personal information that they hold. It also is preferable that a single regime applies to access to, and correction of, personal information in the public and private sector. The 'Access and Correction' principle is discussed in detail in Chapter 29.

15.51 Further, Part V of the FOI Act should be retained. As noted above, the ALRC has received Terms of Reference to review the operation of the FOI Act and related laws. This review could consider amending the FOI Act so that it no longer regulates access to, and correction of, personal information and is limited to regulating access to information about third parties and the deliberative processes of government. The ALRC notes that this model operates effectively under the *Privacy Act 1993* (NZ) and the *Official Information Act 1982* (NZ).[68]

15.52 The FOI Act also could be amended to provide a simpler and more user-friendly process for obtaining access to, and correction of, personal information. Other options for consideration include amendment of the exemptions under the FOI Act to deal with

68 Office of the Privacy Commissioner of New Zealand, *Consultation*, (by telephone), 27 February 2008.

requests to obtain access to personal information and expansion of the correction rights under the FOI Act to accord with those under the *Privacy Act*.[69]

Interaction between the *Privacy Act* and the FOI Act

15.53 While the ALRC is of the view that the current overlap of the access and correction provisions under the *Privacy Act* and the FOI Act should remain, the ALRC has concluded that the provisions that cover the interaction between the *Privacy Act* and the FOI Act require some amendment. In particular, an individual's right to correct his or her personal information under the *Privacy Act* should no longer be subject to the limitations that exist under the FOI Act. This view is reflected in the recommended 'Access and Correction' principle outlined in Chapter 29.

Access provisions

15.54 As noted above, the right of access to personal information under IPP 6 is subject to the exemptions under the FOI Act. In Chapter 29, the ALRC concludes that the exemptions under the FOI Act should apply to agencies when granting access to personal information under the *Privacy Act*. The ALRC expresses the view that individuals should not be able to obtain access to information under the *Privacy Act* that would be the subject of an exemption under the FOI Act. Section 34 reflects this by prohibiting the Privacy Commissioner from providing certain information about documents if they would be exempt documents under the FOI Act.

Correction provisions

15.55 IPP 7.2 provides that the obligation imposed on an agency to correct personal information in IPP 7.1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents. As noted above, the effect of this provision is that the right to correction under IPP 7.1 will be subject to the requirements for an application for correction under Part V of the FOI Act. These requirements are that:

- an individual must have been lawfully provided with the document under the FOI Act or otherwise; and
- the document must have been used, be being used or be available for use, for an 'administrative purpose'.

15.56 The Part also imposes a number of procedural requirements, including: requirements of an application for correction and annotation of records; transfer of requests; and how records are to be corrected, including correction in a way that does not obliterate the text of the record as it existed prior to the correction.[70]

---

69 The difference between the right to correct personal information under the *Privacy Act* and the FOI Act is discussed below.

70 *Freedom of Information Act 1982* (Cth) ss 48–50.

15.57 The ALRC has concluded that an agency's obligation to correct personal information largely should be separated from the limitations outlined under Part V of the FOI Act. These limitations are considered below.

Lawfully provided with the document under the FOI Act or otherwise

15.58 In DP 72, the ALRC expressed the preliminary view that the *Privacy Act* should not provide that lawful access is a prerequisite to the correction of personal information.[71] The OPC submitted that individuals should have the right to request the correction of personal information in an agency's possession regardless of whether access has first been sought formally. This could occur, for example, if an agency sends the individual a letter containing incorrect personal information, such as a misspelled name or address, or containing any number of other types of inaccuracies.[72]

15.59 In ALRC 77, the ALRC and ARC recommended that the requirement of lawful access should be removed from the FOI Act.[73] The ALRC and ARC noted that:

> Access as a prerequisite to seeking amendment or annotation under the FOI Act arises from the fact that amendment rights were first introduced in the FOI Act which deals primarily with access and were regarded as complementary to the right of access. It has been presumed that the only way an individual would know that information was incomplete, incorrect, out of date or misleading would be if they had access to the document.[74]

15.60 The Freedom of Information (Open Government) Bill 2000 (Cth) included an amendment to remove the requirement for lawful access to correct and annotate records under the FOI Act. The Senate Legal and Constitutional Legislation Committee did not support this amendment.[75]

15.61 Lawful access should not be a prerequisite to the correction of an individual's personal information. Lawful access therefore is not a requirement under the recommended 'Access and Correction' principle outlined in Chapter 29. An individual should have a right to insist on correction if they find out by informal means, or reasonably suspect, that personal information is incorrect. There may be situations in which a person legitimately is denied access to a document because it is exempt, but they are sufficiently aware of the contents of the document to know or suspect that it contains false or inaccurate information. The ALRC also notes that lawful access is not a requirement before exercising the rectification right under art 12(b) of the European

---

71 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–9.

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

73 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 77.

74 Ibid, [12.9].

75 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.69]. The Committee did not provide reasons why it did not support this amendment.

Union Directive on the *Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[76]

15.62 The ALRC acknowledges concerns by regulators and law enforcement agencies that such a proposal could enable a person who is the subject of current enforcement action at any stage of that process to demand correction of personal information held by the agency. The ALRC notes, however, that the obligation under the principle is that the agency must take 'reasonable steps' to correct personal information. What is reasonable would depend on the particular circumstances in question.

Administrative purpose

15.63 Under IPP 7.2, the obligation of an agency to correct personal information under IPP 7.1 is subject to the limitation under s 48(b) of the FOI Act. This provides that before a document containing personal information can be corrected, the document must contain personal information about that person that has been used, is being used, or is available for use by the agency or minister for an administrative purpose.

15.64 In *Slezankiewicz v Australian and Overseas Telecommunications Corporation*, Deputy President Thompson stated that 'administrative purpose' means:

> a purpose that has to do with the management of the agency in whose possession a document is held. That management extends at least to all its internal activities, including financial control and activities of an operation nature as well as the employment and management of staff.[77]

15.65 While the ALRC does not recommend that this limitation apply under the 'Access and Correction' principle outlined in Chapter 29, it is the ALRC's view that agencies should not be obliged to correct information that will not be used or disclosed.

15.66 The 'Access and Correction' principle only requires an agency to correct personal information which is, 'with reference to a purpose for which it is held', misleading or not accurate, complete, up-to-date and relevant. In the ALRC's view, the requirement that the information is misleading, not accurate, complete, up-to-date or relevant 'with reference to a purpose for which it is held' would mean that an agency often will not be required to correct personal information that is not being used or disclosed.

Procedural requirements

15.67 As noted above, the obligation of an agency to correct personal information under IPP 7 is subject to various procedural requirements under Part V of the FOI Act. In Chapter 29, the ALRC recommends that the OPC develop and publish guidance on the 'Access and Correction' principle. This guidance should address the requirements

---

76 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).

77 *Slezankiewicz v Australian and Overseas Telecommunications Corporation* [1992] AATA 204, [46].

for an application for correction and annotation of a record, transfer of requests and how records are to be corrected.

Annotation provisions

15.68 IPP 7.3 provides for the annotation of personal information in certain circumstances, subject to the proviso that the personal information has not been amended, wholly or partly, in accordance with an individual's request under the applicable provisions of a law of the Commonwealth. The limitation in IPP 7.3 is reflected in s 35 of the *Privacy Act*, which stipulates when the Privacy Commissioner may annotate personal information following an unsuccessful application under the FOI Act.

15.69 While Part V of the FOI Act remains in operation, an agency's obligation to correct or annotate personal information under the 'Access and Correction' principle should continue to be limited by IPP 7.3 and s 35 of the *Privacy Act*. IPP 7.3 is an appropriate limitation on an agency's obligation to annotate personal information—an agency should not have to annotate personal information if that information has already been corrected, wholly or partly, in accordance with the FOI Act. Section 35 compliments the limitation under IPP 7.3 and should be retained.

15.70 These provisions would not be required if the FOI Act did not regulate the correction of personal information. These provisions should be considered as part of the ALRC's review of the FOI Act and related laws.

Mixed applications

15.71 Applications for access and correction may include a mixture of personal and non-personal information. An agency could deal with such applications solely under the FOI Act, or alternatively, under the *Privacy Act* and the FOI Act. These issues also can be dealt with administratively by agencies—for example, by designing forms to allow for applications relating to personal and non-personal information to be dealt with together. An agency should provide an individual with a 'one stop shop' to obtain access to, and correction of, his or her personal information. The ALRC notes that New Zealand public sector agencies have taken administrative measures to deal with applications for access to documents that include a mixture of personal and non-personal information, and has been advised that this arrangement is working satisfactorily.[78]

Review and complaints

15.72 Under the FOI Act a person may seek internal review and review by the Administrative Appeals Tribunal (AAT) of an agency's decision under the Act not to grant access and amendment of personal information.[79] A complaint about an agency's decision in relation to the access to, and correction of, personal information under the *Privacy Act* are dealt with by the OPC. There currently is no general right of appeal to

78 Office of the Privacy Commissioner of New Zealand, *Consultation*, (by telephone), 27 February 2008.
79 *Freedom of Information Act 1982* (Cth) s 55.

the AAT. Complaints can be made to the Commonwealth Ombudsman about decisions made under both the *Privacy Act* and the FOI Act.

15.73 The OPC generally will decline to investigate a complaint about access to, and correction of, personal information held by an agency if the complainant has not exhausted all FOI Act processes. An applicant therefore will first have to utilise the application processes of the FOI Act and then complain to the Privacy Commissioner if an applicant wishes to seek:

- correction on the grounds that the information is irrelevant;
- deletion of personal information; or
- correction of personal information in a record to which he or she has not been provided lawful access.

15.74 While the Privacy Commissioner has the power to order compensation under the *Privacy Act*,[80] the AAT does not have this power under the FOI Act. If an applicant seeks compensation for a failure by an agency to provide access to, or correction of, personal information, the applicant will have to use the FOI Act to obtain access to, and correction of, the personal information, and then the *Privacy Act* process to seek compensation.

15.75 In DP 72, the ALRC expressed the view that this process is needlessly cumbersome, and that the proposed Part dealing with access to, and correction of, personal information in the *Privacy Act* should provide for a simplified review and complaints mechanism. The ALRC therefore proposed that the Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide for: internal review by an agency of a decision made under the Part; review by the AAT of a decision made under the Part (including the power to make an order for compensation); [81] and complaints to the Commonwealth Ombudsman.[82]

15.76 The ALRC also expressed the preliminary view that the Privacy Commissioner should have an oversight and educational role in relation to access to, and correction of, personal information held by agencies. The ALRC therefore proposed that the OPC should issue guidelines on access to, and correction of, records containing personal information held by an agency.[83]

---

80 *Privacy Act 1988* (Cth) s 52.

81 Decisions of the AAT are reviewable by the Federal Court of Australia: *Administrative Appeals Tribunal Act 1975* (Cth) pt IVA.

82 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–12.

83 Ibid, Proposal 12–13.

Submissions and consultations

15.77 A number of stakeholders supported the proposal.[84] Privacy NSW noted that it mirrored the current review and complaint mechanism under the FOI Act and considered that individuals should be able to seek an internal review.[85] The AAT noted that it already reviews decisions of this kind under the FOI Act, and that it currently has the power to review certain decisions of the Privacy Commissioner under the *Privacy Act*.[86] The AAT submitted that it has the capacity to deal with a jurisdiction of this kind and would not oppose its conferral.[87]

15.78 The OPC supported the right to internal review by an agency, review by the AAT and to lodge a complaint with the Commonwealth Ombudsman regarding the administrative actions of agencies. The OPC submitted, however, that the most appropriate jurisdiction to lodge a complaint regarding an interference with privacy in relation to access to, and correction of, personal information held by an agency would be the OPC.[88]

15.79 PIAC submitted that the legislation should specify clearly whether pursuing one avenue of complaint necessarily rules out another and time limits for carrying out internal review.[89] One stakeholder noted that if application for review by the AAT of any decision by the Privacy Commissioner is to be available, a separate AAT review process as described in the proposal would seem unnecessary.[90]

15.80 The Office of the Victorian Privacy Commissioner (OVPC) suggested that consideration should be given to making the Privacy Commissioner in each jurisdiction the regulator over access to, and correction of, personal information. It noted the New Zealand scheme, under which the Privacy Commissioner and the Ombudsman share the tasks in what may be termed 'information cases'. The OVPC suggested that this type of scheme would mean that the individual's right to obtain access to, and correction of, his or her own information and the process by which this occurs is, as far as possible, the same, regardless of whether it is held in the public or private sector.[91]

15.81 A number of stakeholders, including the OPC,[92] supported the proposal for the OPC to issue guidelines on access to, and correction of, records containing personal information held by an agency.[93] The Australian Federal Police supported the proposal

---

84 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Federal Police, *Submission PR 545*, 24 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

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

86 See, eg, *Rummery and Federal Privacy Commissioner* [2004] AATA 1221.

87 Administrative Appeals Tribunal, *Submission PR 481*, 17 December 2007.

88 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007.

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

90 Confidential, *Submission PR 570*, 13 February 2008.

91 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

93 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.

on the basis that the guidelines were developed in consultation with affected agencies.[94]

ALRC's view

15.82 The same complaint and review mechanisms should apply to agencies as to organisations under the 'Access and Correction' principle. That is, complaint to the OPC and review by the AAT. The current arrangements where complaints may be made to the Ombudsman also should be retained.

15.83 Review and complaints will be dealt with more effectively if the Australian Government establishes a Freedom of Information Commissioner as outlined below. The ALRC is attracted to the arrangement in New Zealand where legislation provides for the body responsible for privacy and the body responsible for freedom of information to refer matters to each other and to consult with each other.[95] This process allows for the body responsible for privacy and the body responsible for freedom of information to consult and consider the views of the other body when dealing with complaints under the relevant legislation. This process would be particularly useful when the Privacy Commissioner and the Freedom of Information Commissioner receive a complaint concerning access to, or correction of, the same personal information or a mixture of personal and non-personal information.

15.84 In the election policy document, *Government Information: Restoring Trust and Integrity*, the Australian Labor Party announced a range of reforms to the FOI Act, including bringing together the functions of privacy protection and freedom of information in an Office of the Information Commissioner. Under this proposal, the existing role of the Privacy Commissioner would be preserved as a statutory office holder responsible for federal privacy laws. A Freedom of Information Commissioner also would be appointed as a statutory office holder responsible for freedom of information law, similar to the Privacy Commissioner. It was further proposed that the Freedom of Information Commissioner would substitute for AAT review of decisions under the FOI Act, with a review lying directly to the Federal Court of Australia or the Federal Magistrates Court.[96] These proposals would also go some way to streamlining the different complaint and review avenues available under the *Privacy Act* and the FOI Act.

Archives Act 1983 (Cth)

15.85 The *Archives Act* establishes the National Archives of Australia (National Archives) and provides for the preservation of the archival resources of the Commonwealth. It also creates an access regime whereby the public generally has a

---

94 Australian Federal Police, *Submission PR 545*, 24 December 2007. See also Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

95 *Privacy Act 1993* (NZ) s 72; *Official Information Act 1982* (NZ) s 29B.

96 K Rudd and J Ludwig, *Government Information: Restoring Trust and Integrity, Election 2007 Policy Document* (2007).

right of access to Commonwealth records that are more than 30 years old (the open access period).[97] The *Archives Act* provides some protection for information relating to the personal affairs of any person (including a deceased person).[98]

15.86 The *Privacy Act* provides that records containing personal information in the custody of the National Archives are subject to the operation of the *Privacy Act*. Two exceptions apply: when the records are in the open access period; or where records are subject to arrangements with a person other than a Commonwealth institution providing for the extent to which the National Archives or other persons are to have access to them.[99] The *Archives Act* controls access to these categories of records.

15.87 While NPP 4 provides that an organisation must take reasonable steps to destroy or permanently de-identify personal information after a certain amount of time, there is no equivalent IPP to govern the retention of records by agencies. Instead, the *Archives Act* regulates the retention of records. It prohibits the destruction of Commonwealth records without the permission of National Archives, subject to some exceptions.[100] The interaction between the *Archives Act* and the 'Data Security' principle is considered in Chapter 28.

The open access period

15.88 In DP 72, the ALRC considered whether the *Privacy Act* should apply to certain classes of records in the open access period for the purposes of the *Archives Act*. The OPC suggested that one option would be to subject Commonwealth records in the open access period to coverage by IPP 11.[101]

15.89 This view was opposed strongly in submissions from federal and state public records authorities.[102] National Archives argued that the exclusion of records in the open access period from the coverage of the *Privacy Act* is a recognition that the sensitivity of much personal information diminishes after 30 years. National Archives noted that extending the coverage of the *Privacy Act* to Commonwealth records in the open access period would limit public access to records, and would impose an unworkable burden on the administration of access by National Archives.[103]

15.90 The ALRC considered this issue in the Report, *Australia's Federal Record: A Review of Archives Act 1983* (ALRC 85) and concluded that the application of the IPPs to records more than 30 years old would be needlessly restrictive. The ALRC stated

---

97 *Archives Act 1983* (Cth) s 31.

98 Ibid s 33. See discussion below.

99 See the definition of 'record' in *Privacy Act 1988* (Cth) s 6. The second exception would relate to, eg, arrangements between individuals to have their personal collections held by National Archives, eg, the 'Whitlam collection' or the 'Fraser collection'.

100 See *Archives Act 1983* (Cth) ss 24–29.

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

102 Queensland Government, *Submission PR 242*, 15 March 2007; National Archives of Australia, *Submission PR 199*, 20 February 2007; Public Record Office Victoria, *Submission PR 72*, 3 January 2007.

103 National Archives of Australia, *Submission PR 199*, 20 February 2007.

that the exemption categories within archives legislation continue to provide appropriate protection for personal information.[104]

15.91 The ALRC affirms that view. The access regime in the open access period must take into consideration the fact that sensitivities attaching to information may diminish after 30 years. Prohibiting the disclosure of all personal information, including names of individuals, would greatly restrict access to archival records.

15.92 The open access period in each state and territory varies. For example, under the *Territory Records Act 2002* (ACT) a record of an agency is open to public access if 20 years has elapsed since the record came into existence.[105] Under the federal *Archives Act*, *State Records Act 1998* (NSW) and the *Public Records Act 1973* (Vic), the open access period is 30 years, and under the *Archives Act 1983* (Tas) it is 25 years.[106] In the interest of national consistency, the Australian Government and state and territory governments, in consultation with the Council of Australasian Archives and Records Authorities, should consider reviewing the *Archives Act* and equivalent state and territory public records legislation to ensure that the 'open access period' under each Act is consistent.

The 'personal affairs' exemption

15.93 Section 33(1)(g) of the *Archives Act* provides an exception to public access to records if the access would involve the unreasonable disclosure of information relating to the 'personal affairs of any person (including a deceased person)'. Section 41 of the FOI Act provides a similar exemption, although it applies to 'personal information' rather than 'personal affairs'.[107]

15.94 'Personal affairs' is generally considered to be a narrower concept than 'personal information'. For example, in *Young v Wicks*, 'personal affairs' was interpreted as 'matters of private concern to a person'.[108] What is critical to the definition of 'personal information' under the *Privacy Act*, however, is that information is capable of identifying an individual rather than its specific nature. Under the current definition of 'personal information',[109] if a person's identity is clear, or reasonably

---

104 Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998), [15.56].

105 *Territory Records Act 2002* (ACT) s 26 provides for this (but is to come into affect on 1 July 2008, according to s 2 of that Act).

106 See, eg, *Archives Act 1983* (Cth) s 31; *State Records Act 1989* (NSW) s 26; *Public Records Act 1973* (Vic) s 10; *Archives Act 1983* (Tas) s 15.

107 See above discussion of *Freedom of Information Act 1982* (Cth) s 41.

108 *Young v Wicks* (1986) 13 FCR 85, 89. See also *Commissioner of Police v District Court of New South Wales* (1993) 31 NSWLR 606, 625; *Colakovski v Australian Telecommunications Corporation* (1991) 29 FCR 429, 436; *Re F and Health Department* (1988) 2 VAR 458, 461.

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

capable of being ascertained, then any information about them is covered, whether or not it is of private concern.[110]

15.95 In DP 72, the ALRC considered whether s 33(1)(g) of the *Archives Act* should be amended to provide an exemption to the unreasonable disclosure of 'personal information' as defined in the *Privacy Act*. The ALRC received only a few submissions on this issue. The OPC submitted that amending the 'personal affairs' exemption to apply to 'personal information' would protect privacy better, and harmonise the *Archives Act* with both the *Privacy Act* and the FOI Act.[111]

15.96 There was strong opposition to such an amendment from other stakeholders.[112] The National Archives submitted that such a proposal would, in practice, unnecessarily restrict access to records, undermining the intent of the *Archives Act*. In addition it would vastly increase the workload of decision makers under the *Archives Act*. National Archives argued that to date the lack of uniformity with the FOI Act terminology has not caused any difficulty in the application of the *Archives Act* or FOI Act. It is appropriate in the context of the different age of the information that it be covered by the two pieces of legislation.[113]

15.97 The ALRC does not make any recommendation in relation to the 'personal affairs' exemption under the *Archives Act*. This position contrasts with that taken by the ALRC in ALRC 85. In that report the ALRC recommended that federal archives legislation should include an exemption category relating to 'personal information', the disclosure of which would, or could reasonably be expected to, have an adverse effect on any person.[114]

15.98 Strong arguments were put forward in submissions against any change to the exemption. The ALRC is concerned that changing the exemption to refer to 'personal information' may needlessly restrict access to records, and undermine the intent of the *Archives Act*. The ALRC is also conscious that such a change would increase the workload of decision makers under the *Archives Act*. The lack of uniformity with the FOI Act terminology has not caused any difficulty in the application of the *Archives Act* and FOI Act, and is an appropriate recognition of the different age and sensitivity of the information covered by the Acts. In the absence of any identifiable problem in this area, the benefits in changing the exemption to refer to 'personal information' do not outweigh the disadvantages of such an amendment.

---

110 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005).

111 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Confidential, *Submission PR 143,* 24 January 2007.

112 Queensland Government, *Submission PR 242,* 15 March 2007; National Archives of Australia, *Submission PR 199,* 20 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

113 National Archives of Australia, *Submission PR 199,* 20 February 2007.

114 Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983,* ALRC 85 (1998), Rec 162.

A single information Act?

15.99 One option for consideration is whether, given the significant overlap between the FOI Act and the *Privacy Act*, the two Acts should be consolidated into a single Act. A number of overseas jurisdictions have combined freedom of information and privacy legislation.[115] The ALRC and the ARC considered this option in ALRC 77 but rejected the proposal on the basis that there was insufficient benefit to outweigh the disadvantage in disturbing the existing legislative framework.[116]

15.100 Another option is to consolidate the FOI Act, the *Privacy Act* and the *Archives Act* into a single Act. An example of such an Act is the *Information Act 2002* (NT). The ALRC and the ARC also considered this option in ALRC 77. The option met with strong opposition from stakeholders, however, and was ultimately rejected. The ALRC and ARC recommended instead that the *Privacy Act*, FOI Act and *Archives Act* be amended, where necessary, to provide a cohesive and consistent package of legislation on government records.[117]

15.101 There was little support for combining the *Privacy Act*, FOI Act and *Archives Act* in submissions to this Inquiry. Stakeholders noted that the three Acts have different purposes, and considered that the ALRC should focus on the harmonisation of the Acts.[118]

15.102 Despite their many common aspects, each Act has a distinct purpose that is understood by agencies and the public. There is insufficient benefit in combining the two Acts to outweigh the disadvantage in disturbing the current legislative framework. In particular, the fact that the *Privacy Act* regulates both the public and private sectors detracts from the appeal of a single Act.

15.103 One option that may address the interaction of the three Acts is to clarify the objects of each Act. In Chapter 3, the ALRC recommends that the *Privacy Act* be amended to include an objects clause. In ALRC 77, the ALRC and the ARC recommended the amendment of the FOI Act's objects clause and, in ALRC 85, the ALRC proposed an amendment of the *Archives Act* to include an objects clause.[119]

---

115 See, eg, *Freedom of Information and Protection of Privacy Act 1990* RSO c F 31 (Ontario) and *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia).

116 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [5.19].

117 Ibid, [5.6].

118 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; National Archives of Australia, *Submission PR 199*, 20 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Confidential, *Submission PR 143*, 24 January 2007; Public Record Office Victoria, *Submission PR 72*, 3 January 2007.

119 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 4 and Rec 1; Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998), Ch 4 and Rec 1.

A single regulator?

15.104 One issue for consideration is whether the same body should administer the *Privacy Act* and the FOI Act. This is the case in the Northern Territory[120] and a number of overseas jurisdictions, for example British Columbia, Ontario, and the United Kingdom.[121]

15.105 While the ALRC notes that the combination of these roles appears to work effectively in other jurisdictions, the ALRC does not recommend the establishment of a single body to administer the *Privacy Act* and the FOI Act. There was little support for such a change. Some stakeholders noted that the *Privacy Act* and the FOI Act have different focuses, and so should be administered by two different bodies.[122]

15.106 The Australian Government should, however, establish a body to oversee the administration of the FOI Act. A number of stakeholders supported a separate body, such as an Information Commissioner, to oversee freedom of information at the federal level.[123] As outlined in DP 72, in the ALRC's view it would be appropriate to confer the functions of the Freedom of Information Commissioner on the Commonwealth Ombudsman.[124]

15.107 As noted above, the Australian Government's election policy document *Government Information: Restoring Trust and Integrity* sets out the Government's proposals for a restructure of freedom of information laws.[125] These proposals include bringing together the functions of privacy protection and freedom of information in an Office of the Information Commissioner. The Office of the Information Commissioner would act as a whole-of-government clearinghouse for complaints, oversight, advice and reporting for freedom of information and privacy matters. Under this proposal, the existing role of the Privacy Commissioner would be preserved as a statutory office holder responsible for federal privacy laws. A Freedom of Information Commissioner would also be appointed as a statutory office holder responsible for freedom of information law, similar to the Privacy Commissioner.

---

120 See Ch 2.

121 See Office of the Information and Privacy Commissioner for British Columbia, *Website* <www.oipcbc.org> at 30 July 2007; Ontario Information and Privacy Commissioner, *Website* <www.ipc.on.ca> at 30 July 2007; United Kingdom Government Information Commissioner's Office, *Website* <www.ico.gov.uk> at 30 July 2007.

122 Confidential, *Submission PR 143,* 24 January 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

123 Australian Government Department of Human Services, *Submission PR 541,* 21 December 2007; Smartnet, *Submission PR 457,* 11 December 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

124 Australian Law Reform Commission, *Review of Australian Privacy Law,* DP 72 (2007), [12.103]–[12.104]. Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), 58.

125 K Rudd and J Ludwig, *Government Information: Restoring Trust and Integrity, Election 2007 Policy Document* (2007).

15.108 While the ALRC does not recommend a single regulator to administer the *Privacy Act* and the FOI Act, the ALRC notes that the Government's proposal for an Office of the Information Commissioner is not inconsistent with any of the ALRC's recommendations in this Report. In particular, the ALRC notes that the Government's policy maintains a separate focus for the Privacy Commissioner and a Freedom of Information Commissioner. The ALRC also notes the advantages of having the Privacy Commissioner and a Freedom of Information Commissioner co-located in a single office to deal with complaints about access, particularly when a document contains a mixture of personal and non-personal information.

Secrecy provisions

15.109 Federal legislation contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office. Secrecy provisions usually are based on the need to preserve the secrecy of government operations in order for government to function effectively.

15.110 The secrecy interests of agencies and the privacy interests of individuals will sometimes be complementary. For example, both an agency and the subject of information held by the agency might have an interest in non-disclosure of that information to third parties. Those interests, however, may sometimes conflict. For example, a person may want access to his or her personal information to check that it has been recorded correctly and is not being disclosed without his or her consent; but to grant that access could intrude upon the secrecy interests of the agency.

15.111 There are a number of provisions in federal legislation that create general offences in relation to the unauthorised disclosure of official information.[126] There are also secrecy provisions in federal legislation that deal with unauthorised disclosure of information in specific circumstances.[127] Secrecy provisions in federal legislation create criminal offences that attract criminal penalties. The *Privacy Act*, however, operates as an administrative regime that allows for private remedies such as the award of compensation.[128]

---

126 See, eg, *Crimes Act 1914* (Cth) ss 70 and 79; *Criminal Code* (Cth) s 91.1.

127 See, eg, *Inspector-General of Taxation Act 2002* (Cth) s 37(1); *Gene Technology Act 2000* (Cth) s 187(1); *Aged Care Act 1997* (Cth) s 86-2; *Australian Prudential Regulation Authority Act 1998* (Cth) ss 5, 56; *Australian Postal Corporation Act 1989* (Cth) s 90H; *Civil Aviation Act 1988* (Cth) s 32AP(1); *Australian Institute of Health and Welfare Act 1987* (Cth) s 29(1); *Disability Services Act 1986* (Cth) s 28(2); *Australian Security Intelligence Organisation Act 1979* (Cth) s 92. In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs reported that there were more than 150 secrecy provisions in federal legislation and more than 100 different statutes that contain such provisions: 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), xxiv.

128 *Privacy Act 1988* (Cth) pt IIIA creates a range of credit reporting offences: see Part G. The ALRC recommends that the *Privacy Act* be amended to provide for civil penalties in limited circumstances: see Rec 50–2.

15.112 As noted above, the *Privacy Act* includes exceptions to some of the IPPs if acts or practices are required or authorised by or under law. Secrecy provisions that prevent disclosure of information will be consistent with IPP 6 as that principle provides an exception for record-keepers that are required or authorised by a federal law to refuse to provide an individual with access to a record.[129] Further, secrecy provisions that provide for disclosure of protected information in certain circumstances will be consistent with IPP 11, as the disclosure is required or authorised by or under law.[130] The exception under IPP 11.1(e) in relation to law enforcement, the enforcement of a pecuniary penalty or the protection of the public revenue also may be relevant in some contexts.[131]

15.113 In 2006, the *Privacy Act* was amended to insert a new Part VIA into the Act.[132] The object of the Part is to make special provision for the collection, use and disclosure of personal information in emergencies and disasters. Section 80P(1) provides that at any time when an emergency declaration is in force in relation to an emergency or disaster, an entity may collect, use or disclose personal information in certain circumstances. Section 80P(2) provides that an entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by s 80P(1), unless the secrecy provision is a 'designated secrecy provision'. Designated secrecy provisions include provisions under the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth).[133]

15.114 A number of reviews have considered secrecy provisions in federal legislation.[134] For example, the ALRC considered secrecy provisions in its report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98). The ALRC made a number of recommendations, including that the Australian Government should undertake a review of federal secrecy provisions.[135]

15.115 In DP 72, the ALRC considered whether the various secrecy provisions under federal legislation that prohibit Commonwealth public servants from disclosing information contribute to inconsistency and fragmentation in personal information privacy regulation. In particular, the ALRC considered whether the *Privacy Act*, rather than secrecy provisions in specific statutes, should regulate the disclosure of personal information by Australian Government agencies.

---

129 Ibid s 14, IPP 6.

130 Ibid s 14, IPP 11.1(d).

131 Taxation legislation includes a number of secrecy provisions which may be said to authorise disclosure of information for the protection of public revenue. See M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt I)' (2002) 8 *Privacy Law & Policy Reporter* 181; M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt II)' (2002) 8 *Privacy Law & Policy Reporter* 193.

132 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth). The Part commenced operation on 7 December 2006.

133 See *Privacy Act 1988* (Cth) s 80P(7).

134 For example, 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);

135 See Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Ch 5, Recs 5–1 to 5–5.

15.116 The ALRC also considered whether there is a need to clarify the relationship between the *Privacy Act* and other legislation containing secrecy provisions. Some secrecy provisions address the operation of the *Privacy Act*.[136] Other provisions, however, do not address this issue.[137]

15.117 A number of government agencies noted that they are subject to secrecy provisions, and that the provisions work well.[138] There was no support for having the *Privacy Act*, rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by Australian Government agencies.[139] In particular, it was noted that the use of specific statutes allows secrecy provisions to be tailored to particular types of protected information and the situation of the agency,[140] and that protecting all personal information under the *Privacy Act* would not, in some circumstances, provide the level of protection that may be necessary.[141]

15.118 It was also noted in submissions that secrecy provisions can apply to information that includes, but is not limited to, 'personal information', enabling a wider range of information to be protected.[142] The Australian Government Department of Health and Ageing noted that providing offences in the *Privacy Act* could be seen as contrary to the 'light-touch' approach that has underpinned the regulation of privacy under the *Privacy Act* to date.[143] The OPC submitted that it was not appropriate for the Privacy Commissioner to administer and enforce secrecy laws.[144]

15.119 In DP 72, the ALRC did not make any proposals in relation to secrecy provisions, and expressed the preliminary view that information that is currently protected by various secrecy provisions in federal legislation should not be regulated

---

136 See, eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 5(12). The section also contains a note: 'For additional rules about personal information, see the *Privacy Act 1988* (Cth)'.

137 See, eg, *Disability Services Act 1986* (Cth) s 28.

138 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007.

139 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007.

140 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007.

141 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

142 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

143 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

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

by the *Privacy Act*. The ALRC also stated that secrecy provisions in federal legislation should be reviewed, noting that the need for this review has been established by a number of inquiries. No submissions on secrecy provisions were received in response to the views expressed in DP 72.

15.120 Information that is currently protected by secrecy provisions in federal legislation should not be regulated by the *Privacy Act*. In the ALRC's view, it is appropriate that specific statutes include secrecy provisions designed to protect information. This ensures that an agency's secrecy responsibilities are tailored to the agency's circumstances and grouped with its other obligations.

15.121 Secrecy provisions do not relate solely to personal information. They also protect, for example, commercial, security and operational information. Secrecy provisions provide separate and specific standards of protection beyond those afforded by the privacy principles under the *Privacy Act*. Unlike the privacy principles, the level of protection afforded by secrecy provisions will often vary with the sensitivity of the information concerned.

15.122 The ALRC acknowledges, however, that secrecy provisions may affect adversely the privacy interests of an individual. The ALRC is of the view, therefore, that a privacy impact assessment (PIA) should be prepared when a secrecy provision is proposed in new legislation that may have a significant impact on the handling of personal information.[145] PIAs are discussed in Chapter 47. Further, where a secrecy provision regulates personal information, that provision should address how the requirements under the provision interact with the privacy principles in the *Privacy Act*.

15.123 Secrecy provisions in federal legislation should be reviewed. The need for this review has been established by a number of ALRC inquiries. In ALRC 77, the ALRC recommended that

> a thorough review of all federal legislative provisions that prohibit disclosure by public servants of government held information should be conducted as soon as possible to ensure that they do not prevent the disclosure of information that would not be exempt under the FOI Act.[146]

15.124 As noted above, in ALRC 98 the ALRC also recommended a review of secrecy provisions to ensure that each provision is consistent with the *Australian Constitution* and to consider the lack of consistency in the fundamental principles and penalty structures in the provisions.[147] The Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.

---

145 See Proposal 47–4.

146 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 4, Rec 13. See also Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1320].

147 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Ch 5, Rec 5–2.

Recommendation 15–2 The Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.

Obligations of confidence

Common law and equitable duties of confidence

15.125 Legally enforceable obligations to maintain confidence may arise in contract and equity. These obligations are capable of applying to individuals, organisations, agencies and officers of agencies.[148] Relief is available against third party recipients of confidential information, and those who knowingly assist a confidant to breach his or her obligations of confidentiality.[149]

15.126 A contractual obligation of confidence can arise from express terms in a contract, but also by implication.[150] The nature of the obligation will depend on the terms of the contract. Remedies for threatened and actual breach of the contractual obligations to maintain confidence include injunctions and damages.

15.127 An equitable obligation of confidence can arise where the formalities for the formation of a contract are not present.[151] The obligation arises where information with the necessary quality of confidence is imparted in circumstances importing an obligation of confidence.[152] Such circumstances will exist where the information is imparted on the understanding that it is to be treated by the confidant on a limited basis, or where the confidant ought to have realised that in all the circumstances the information was to be treated in such a way.[153] Breach of the obligation occurs where there is an unauthorised *use*, not only where there is unauthorised *disclosure*, of the information.

15.128 Unlike the position in contract, where loss is the basis of a claim for damages, the plaintiff in a suit for breach of the equitable obligation does not need to show any

148 See, eg, *Johns v Australian Securities Commission* (1993) 178 CLR 408, 459–460; *Attorney-General (UK) v Heinemann Publishers Pty Ltd* (1987) 10 NSWLR 86, 191 (McHugh JA).

149 *Johns v Australian Securities Commission* (1993) 178 CLR 408, 459-460; *Breen v Williams* (1996) 186 CLR 71, 129; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [137].

150 *Parry-Jones v Law Society* [1968] 1 All ER 177; R Meagher, J Heydon and M Leaming, *Meagher Gummow & Lehane's Equity: Doctrines & Remedies* (4th ed, 2002), [41–015].

151 Ibid, [41–020].

152 *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic)* (1987) 14 FCR 434, 443; *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* (1990) 22 FCR 73, 86–87.

153 *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* (1990) 22 FCR 73, 86–87; *Coulthard v State of South Australia* (1995) 63 SASR 531, 546–547.

damage.[154] Remedies for breach of the equitable obligation include compensation or an account of profits, an injunction and a declaration.

Statutory protection of confidential information

15.129 Legally enforceable obligations of confidence also may arise under statute. The FOI Act, for example, addresses government confidentiality and provides that a document is an exempt document if its disclosure under the FOI Act would found an action, by a person (other than an agency or the Commonwealth), for breach of confidence.[155] Federal, state and territory legislation also include a number of confidentiality provisions.[156]

Part VIII of the *Privacy Act*

15.130 Part VIII of the *Privacy Act* applies where an agency or an employee of an agency (a 'confidant') is subject to an obligation of confidence to another person (a 'confider') in respect of personal information.[157]

15.131 The obligation applies whether or not the information relates to the confider or to a third person.[158] It generally preserves all other laws, principles or rules 'under or by virtue of which an obligation of confidence exists', except as expressly qualified, or by necessary implication. It also preserves laws, principles or rules that 'have the effect of prohibiting, or imposing a liability (including a criminal liability) on a person in respect of, a disclosure or use of information'.[159] Part VIII, therefore, allows for the fact that obligations of confidence may arise in various ways.

15.132 The operative provisions of Part VIII are ss 92 and 93. Section 92 extends the obligation a confidant owes to a confider to a third party who acquires the information knowing, or being in a position where he or she ought reasonably to know, that the person from whom he or she acquired the information was subject to an obligation of confidence. Section 93 concerns relief for breach of the obligation. Without limiting any other right a confider has to relief in respect of a breach,[160] a confider under s 93(1) 'may recover damages from a confidant in respect of a breach of an obligation of confidence with respect to personal information'.[161]

---

154 *National Roads and Motorists' Association Ltd v Geeson* (2001) 40 ACSR 1, [58]; *NP Generations Pty Ltd v Feneley* (2001) 80 SASR 151, [21].

155 *Freedom of Information Act 1982* (Cth) s 45.

156 See discussion of *Privacy Act 1988* (Cth) pt 8 below and discussion of other confidentiality provisions in Chs 16, 60.

157 The history of Part VIII of the *Privacy Act* is outlined in Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [12.129]–[12.130].

158 *Privacy Act 1988* (Cth) s 90.

159 Ibid s 91.

160 Ibid s 93(2).

161 Since s 93(1) does not limit or restrict any other right that the confider has in respect of the breach, he or she will continue to have a claim to the remedy of equitable compensation where the obligation arises in the equity jurisdiction rather than, for example, in contract. The assessment of 'damages' under s 93(1) will not necessarily use the same criteria of quantum, causation, remoteness etc as those that apply to assessment of equitable compensation, or to assessment of damages in contract or for any other civil wrong.

15.133 Where the information the subject of the confidence is personal information relating to a third person, that person 'has the same rights against the confidant in respect of a breach or threatened breach of the obligation as the confider has'.[162] This is an important extension of the general law position.

15.134 Courts of the ACT are conferred with jurisdiction regarding matters arising under Part VIII, although this does not deprive 'a court of a State or of another Territory of any jurisdiction that it has'.[163] There are no known court decisions (reported or unreported) applying the confidentiality provisions.

15.135 In DP 72, the ALRC considered whether the provisions in Part VIII of the *Privacy Act* are adequate and necessary and, if so, whether the provisions should be contained in the *Privacy Act* or elsewhere. The ALRC noted that Part VIII represents an extension of the law of confidentiality in that it extends the right to enforce a duty of confidentiality to the person to whom the information relates. The ALRC expressed the view that rather than extending the law of confidentiality, it is more appropriate to enact a statutory cause of action for a serious invasion of privacy.[164] The ALRC proposed therefore that Part VIII of the *Privacy Act* should be repealed.[165]

15.136 All stakeholders that addressed the issue supported the proposal that Part VIII should be repealed.[166] For example, the OPC submitted that it was persuaded by arguments of the ALRC that the Part is unnecessary, given the proposal of a statutory cause of action for a serious breach of privacy.[167]

15.137 The confidentiality provisions contained in Part VIII of the *Privacy Act* should be repealed. The ALRC notes that the provisions have never been used. It is hard to imagine when this action would be used in preference to making a complaint to the OPC about a breach of the IPPs (or the model Unified Privacy Principles (UPPs)).

15.138 As noted above, Part VIII represents an extension of the law of confidentiality in that it extends the right to enforce a duty of confidentiality to the subject of the information. This right is not available under Australian common law.[168]

15.139 As discussed in Part K, the United Kingdom (UK) courts have developed the action for breach of confidence so that it now covers the wrongful disclosure of private information.[169] The ALRC agrees with the views expressed by the New South Wales Law Reform Commission (NSWLRC) that the law in Australia relating to breach of

---

162 *Privacy Act 1988* (Cth) s 93(3).
163 *Privacy Act 1988* (Cth) s 94.
164 The ALRC's recommendations for a statutory cause of action are outlined in Ch 74.
165 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 12–14.
166 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; Australia Post, *Submission PR 445*, 10 December 2007.
167 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
168 *Commonwealth v John Fairfax & Sons Ltd* (1980) 147 CLR 39, 51.
169 See *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920; *Ash v McKennitt* [2007] 3 WLR 194.

confidence should not follow the UK case law. The NSWLRC has listed three reasons why such a change is undesirable:

> First, confidentiality and privacy are simply different concepts … While most confidential acts and information could arguably be described as private, not all private activity is necessarily confidential.
>
> Secondly, the doctrine of breach of confidence, developed primarily in the exclusive jurisdiction of equity, seems an unsuitable vehicle for the introduction and development of greater privacy protection … equitable intervention does not fasten on the intrinsic value of the information itself.
>
> Thirdly, although the legal notion of confidence is not necessarily restricted to the disclosure of 'information' in any technical sense, it is unclear to what extent breach of confidence would be useful beyond situations involving the unjustified publication of private information.[170]

15.140 Rather than extending the law of confidentiality, it is more appropriate to enact a statutory cause of action for a serious invasion of privacy. The cause of action will apply both to agencies and organisations, unlike Part VIII which only applies to agencies; will provide broader protection of privacy than that offered by Part VIII; and will offer a range of remedies. The ALRC's recommendation for a statutory cause of action for a serious breach of privacy is outlined in Chapter 74.

Recommendation 15–3 Part VIII of the *Privacy Act* (Obligations of confidence) should be repealed.

170 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007).

16. Required or Authorised by or Under Law

Contents

Introduction

16.1 An act or practice 'required or authorised by or under law' is an exception to a number of the limits on the handling of personal information under the *Privacy Act 1988* (Cth). This chapter first considers what is meant by the phrase 'required or authorised by or under law', and considers whether the model Unified Privacy Principles (UPPs) should include a new exception for acts and practices that are 'specifically authorised by or under law'. The chapter then considers a number of federal Acts that require or authorise acts and practices for the purposes of the *Privacy Act*. These include the *Census and Statistics Act 1905* (Cth), the *Corporations Act 2001* (Cth), the *Commonwealth Electoral Act 1918* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act).

'Required or authorised by or under law'

16.2 An act or practice 'required or authorised by or under law' is an exception (the 'required or authorised exception') to a number of the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs).[1] For example, IPP 11(1)(d) provides that a record-keeper may disclose personal information to a person, body or agency if the disclosure is required or authorised by or under law. NPP 2.1(g) similarly provides that an organisation may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by or under law. The required or authorised exception also applies to other areas of the *Privacy Act*, such as credit reporting.[2]

16.3 The ALRC recommends that acts or practices that are required or authorised by or under law should be an exception to a number of the model UPPs, including the 'Collection', 'Use and Disclosure', 'Data Security', 'Access and Correction' and the 'Cross-border data flow' principles. It is also referred to in the 'Notification' principle.[3]

16.4 State and territory privacy laws include similar exceptions. For example, s 25 of the *Privacy and Personal Information Protection Act 1998* (NSW) provides that it is an exception to various Information Privacy Principles under that Act if an agency is 'lawfully authorised or required not to comply with the principle concerned', or 'non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law'.[4]

Scope of the exception

'Required' by or under law

16.5 The Office of the Privacy Commissioner (OPC) states that an agency should inform an individual that it is 'required' to collect personal information in accordance with IPP 2 only 'in the rare case where the agency has no choice in whether or not it collects the information'.[5] This interpretation is consistent with interpretations of

---

1 *Privacy Act 1988* (Cth) s 14, IPPs 5.2, 6, 10.1(c), 11.1(d); sch 3, NPPs 2.1(g), 6.1(h) and 10.2(b)(i).

2 See, eg, Ibid ss 6D(7)(b), 18L.

3 In Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), the 'Notification' principle was referred to as the 'Specific Notification' principle—the name of the principle has now changed: see Ch 23. The 'Data Security' principle and the 'Cross-border Data Flows' principle now include a 'required or authorised by law' exception. It was not proposed in DP 72 to include the exception in these principles.

4 See also Principle 9 in the *Health Records (Privacy and Access) Act 1997* (ACT) which provides for an exception to the use of personal health information if the use is required or authorised by a law of the ACT, a law of the Commonwealth, or an order of a court of competent jurisdiction. Similarly, Health Privacy Principle 2 (Use and Disclosure) of the *Health Records Act 2001* (Vic) provides an exception for uses and disclosures that are 'required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law)'.

5 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 21. See also *Re VBN and Australian Prudential Regulation Authority* (2006) 92 ALD 475, [38].

'required' in the context of other laws.[6] For example, in *Department of Premier & Cabinet v Hulls*, the Victorian Court of Appeal found that 'required' meant 'demands' or 'necessitates'.[7]

16.6 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that the use of the word 'required' in NPP 2.1(g) is intended to cover situations where a law unambiguously requires a certain act or practice. It also suggests, however, that a law could require an act or practice by implication.

> 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.[8]

16.7 The interpretation of 'required by law' seems to be consistent across the NPPs and IPPs. In relation to NPP 2.1(g) (Use and disclosure), the OPC states that 'required by law' covers 'circumstances in which there is a legal obligation to use or disclose personal information in a particular way'.[9] Examples provided by the OPC of when the use or disclosure of personal information is required include where there are statutory requirements to report matters to agencies or enforcement bodies, or where legislation requires an organisation to 'carry out some action, which of necessity involves particular uses or disclosures of personal information'.[10] This is reflected in *Rahman v Ashpole*,[11] in which Graham J held that disclosure of personal information by a bank to Centrelink was required or authorised by or under the provisions of the *Social Security (Administration) Act 1999* (Cth).[12]

16.8 The OPC suggests a similar interpretation of 'required by law' in relation to IPP 10 (Limits on use of personal information). The OPC states that an agency may be required by law to use personal information for another purpose if it is governed by legislation that requires it to perform a specific function, and the only possible way it can perform that function is by using the particular information for a purpose other than that for which it was obtained.[13] In the context of IPP 11, Commonwealth tribunals have held that there is no reason to depart from the ordinary meaning of the

---

6 See, eg, *Chamberlain v Banks* (1985) 7 FCR 598, [14] (*Administrative Decisions (Judicial Review) Act 1977* (Cth) s 5(1)(b)); *Department of Premier & Cabinet v Hulls* [1999] 3 VR 331, [31] (*Freedom of Information Act 1982* (Vic) s 50(4)).

7 *Department of Premier and Cabinet v Hulls* [1999] 3 VR 331, [358].

8 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 139.

9 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001), 2.

10 Ibid, 2.

11 *Rahman v Ashpole* [2007] FCA 1067.

12 Ibid, [19].

13 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), 42.

term 'require'; that is, 'to demand, exact or command by authority' or 'to have as a necessary or essential condition for success, fulfilment, etc'.[14]

16.9 The *Guidelines to the Information Privacy Principles*, issued by the Office of the Victorian Privacy Commissioner (OVPC), state that:

> words such as 'must' or 'shall' will indicate a requirement, and may be accompanied by the presence of a sanction for non-compliance.[15]

16.10 The guidelines list warrants, court orders and statutory provisions as examples.

'Authorised' by or under law

16.11 While an agency or an organisation that is 'required' by law to engage in an act or practice has no choice in the matter, an agency that is 'authorised' by law has a discretion as to whether it will engage in an act or practice.[16] The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that the reference to 'authorised', 'encompasses circumstances where the law permits, but does not require, use or disclosure'. [17]

16.12 In the opinion of the OPC, an act or practice is not 'authorised' solely because there is no law prohibiting it.[18] Further, the law that authorises an act or practice must provide a 'specific relevant discretion'. For example, a general provision that a statutory office-holder or the head of an agency may do anything necessary or convenient to be done for, or in connection with, a function does not meet this criterion.[19]

16.13 Sometimes, authorisation will be express. For example, s 250–10 of the *Private Health Insurance Act 2007* (Cth) provides that, under certain circumstances, disclosure of personal information to the Private Health Insurance Ombudsman is taken to be authorised by law under the *Privacy Act.*[20] A law also can impliedly 'authorise' an act or practice.

16.14 Again, the interpretation of the phrase 'authorised by law' has been consistent across the IPPs and NPPs. The OPC has stated in the context of the required or authorised exception to IPP 10 and IPP 11:

> A use or disclosure may fall within 10.1(c) or 11.1(d) if the law requires or authorises a function or activity that clearly and directly entails the use or disclosure. Here, the

---

14 *Skase and Minister for Immigration and Multicultural and Indigenous Affairs* [2005] AATA 200 [34]–[35]. See also *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83, [37] and *VBN v Australian Prudential Regulation Authority* (2006) 92 ALD 475, [38].

15 Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles* (2nd ed, 2006), [2:118]. The Guidelines refer to a decision of the Victorian Court of Appeal in *Department of Premier and Cabinet v Hulls* [1999] 3 VR 331, [358], referred to above.

16 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), 42.

17 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [358].

18 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), 43.

19 Ibid, 42–3.

20 *Private Health Insurance Act 2007* (Cth) s 250-10.

> use or disclosure is impliedly authorised by law because it is essential to effect a scheme the law lays down.[21]

16.15 In the context of IPP 11, as with the term 'required', Commonwealth tribunals have held that there is no reason to depart from the ordinary meaning of the term 'authorised'; that is, 'to give someone the power or right to do something' or 'to give permission for something'.[22] In *Caratti v Commissioner of Taxation*,[23] French J held that it was within the course of duties of an officer of the Australian Taxation Office (ATO) to disclose to the Director of Public Prosecutions information relevant to possible criminal proceedings. French J found that the disclosure fell within the required or authorised exception and so did not contravene IPP 10 or IPP 11.

> I accept the Commissioner's submissions that on the face of the pleading any disclosures made by the Commissioner … of information obtained in the course of the taxation audits or otherwise under the Act, the *Taxation Administration Act* or the *Fringe Benefit Tax Assessment Act 1986*, which contains similar provisions, were permitted by the statutory provisions and were not made in contravention of them.[24]

16.16 The OPC has provided similar guidance on the meaning of the term 'authorised' in the context of the NPPs—namely, that it means there is authority to do something but the organisation can decide whether or not to do it.[25] In the context of NPP 2.1(g), Wilson FM in the Federal Magistrates Court has held that the disclosure of documents that contained personal information, but which also contained information relevant to the investigation of the receipt of 'income', was 'authorised' for the purposes of the *Privacy Act* by s 77A of the *Bankruptcy Act 1966* (Cth), but only to the extent that the documents were relevant to the trustee's investigation.[26] Wilson FM held that if the necessary financial information could be provided to the trustee, without disclosure of 'personal information', that would constitute sufficient compliance by the respondent with the trustee's request under s 77A of the *Bankruptcy Act 1966* (Cth).[27]

16.17 The *Guidelines to the Information Privacy Principles*, issued by the OVPC, state that words such as 'may' are indicative of authorisation. The Guidelines provide that 'an authorising power must be reasonably specific; a general power or function for "anything incidental" would be insufficient'.[28]

---

21 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), 43.

22 *Skase and Minister for Immigration and Multicultural and Indigenous Affairs* [2005] AATA 200 , [34]–[35]. See also *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83, [37] and *VBN v Australian Prudential Regulation Authority* (2006) 92 ALD 475, [38].

23 *Caratti v Federal Commissioner of Taxation (Cth)* (1999) 99 ATC 5044.

24 Ibid, [27]. Note that the Act referred to by French J is the *Income Tax Assessment Act 1936* (Cth).

25 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41 (IPP 2.1(g)) and 51 (IPP 6.1(h)).

26 *Fletcher v EEBME Pty Ltd* (2007) 213 FLR 1, [31].

27 Ibid, [31].

28 Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles* (2nd ed, 2006), [2:120].

'By or under law'

16.18 In *Scott v Enfield City*, Wells J explained the distinction between 'by or under' law as follows:

> The word 'by' implies, I apprehend, that the use or intended use belonged to a class of use directly permitted by a provision or provisions of the Act or bylaw; the word 'under' implies that the authorization of the use or intended use was an act-in-law validly done pursuant to the Act or by–law.[29]

16.19 In *R v Tkacz*, however, Malcolm CJ acknowledged that while, in particular contexts, a distinction can be made between 'by' and 'under', there are other contexts where they have the same meaning.[30]

'Law'

16.20 What kinds of laws can require or authorise acts or practices for the purposes of the exception? Only a few cases have considered what is meant by 'law' for the purposes of the 'required or authorised' exception. It has been held that 'law' in the context of the exception includes a federal Act[31] and court rules.[32]

16.21 The OPC's *Guidelines to the National Privacy Principles* provide that 'law' includes Commonwealth, state and territory legislation, as well as common law.[33]

16.22 The OPC's *Plain English Guidelines to the Information Privacy Principles* provide more detailed advice on the meaning of 'law'. They provide that 'law' for the purposes of the required or authorised exception to IPP 10 and IPP 11 means Commonwealth acts and delegated legislation, and state and territory laws where the state or territory has 'validly legislated to bind the Commonwealth'.[34] The Guidelines also state that 'law' includes:

- documents with the force of Commonwealth law (a document may have the 'force of law' if it is an offence to breach its provisions, or it is possible for a penalty lawfully to be imposed if its provisions are breached, for example, industrial awards);
- disclosures to Commonwealth ministers; and
- Commonwealth parliamentary privilege.[35]

16.23 The OPC states that a number of laws normally are not accepted as 'law' for the purpose of the required or authorised exception, including:

---

29 *Scott v Enfield City* (1982) 49 LGRA 301, 305.
30 *R v Tkacz* [2001] 25 WAR 77, [23] – [26].
31 *Re VBN and Australian Prudential Regulation Authority* (2006) 92 ALD 475, [39].
32 *Re An Application by the NSW Bar Association* [2004] FMCA 52, [5]–[6].
33 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41.
34 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), 40.
35 The OPC notes, however, that if the *Privacy Act* would prohibit the disclosure, were it not for parliamentary privilege, it may be appropriate for the agency to approach its minister with any concerns it has about disclosing the personal information: Ibid.

- state law that does not validly bind the Commonwealth;
- Cabinet decisions;
- inter-agency agreements and contracts between an agency and other parties;
- common law; and
- requests for personal information from foreign governments.[36]

16.24 Common law, for these purposes, 'consists of broad statements of legal principle and is made by judges—as opposed to statute law which is legislation made by Parliament'.[37]

16.25 In the second reading speech for the Privacy Amendment (Private Sector) Bill 2000, the then Attorney-General stated that the 'national privacy principles recognise the operation of state and territory legislation and the common law'.[38]

16.26 State and territory courts and tribunals have held that the meaning of 'law' in relation to similar exceptions under state and territory privacy laws: includes a common law duty of care to warn;[39] an order for pre-trial discovery;[40] a subpoena to disclose information to a court;[41] and a warrant to obtain records from a hospital under a state Act.[42] In its submission to the NSW Attorney General's Department review of the *Privacy and Personal Information Protection Act 1998* (NSW), the Office of the NSW Privacy Commissioner (Privacy NSW) stated that the scope of 'other law' in s 25 of the Act was unclear.[43]

Clarifying the scope of the exception

Clarifying the scope of 'law'

16.27 In the Discussion Paper, *Review of Privacy Law* (DP 72), the ALRC expressed the preliminary view that the scope of the required or authorised exception required clarification.[44] It noted that some stakeholders had expressed concern that the ambiguity in the operation of this exception can create uncertainty for individuals, agencies, organisations and privacy regulators.

---

36 These requests will only fall within the exceptions in IPP 10.1(c) or 11.1(d) if there is a Commonwealth law that requires or authorises the agency to provide personal information in those circumstances. Similarly, treaty obligations only fall within these exceptions if there is a Commonwealth law that enacts the obligation: Ibid, 41.

37 Ibid, 41.

38 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15751–2.

39 *Director General Department of Education and Training v MT* [2005] NSWADTAP 77, [83].

40 *Grant v Marshall* [2003] FCA 1161, [4].

41 *HW v Commissioner of Police* [2003] NSWADT 214, [63]–[64].

42 *Royal Women's Hospital v Medical Practitioners Board of Victoria* (2006) 15 VR 22, [132]–[134].

43 Privacy NSW, *Submission to the New South Wales Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998*, 24 June 2004, 88.

44 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.29].

16.28 The ALRC stated that while the scope of the words 'required' and 'authorised' appear to be well understood, the categories of laws that are 'law' for the purposes of the exception were less clear.

16.29 The ALRC expressed the preliminary view that federal Acts and delegated legislation are clearly 'law' for the purpose of the exception. These laws are subject to various accountability requirements, including the scrutiny of Parliament and disallowance. These accountability requirements help to ensure that any reliance on the required or authorised exception is appropriate and justified.

16.30 The ALRC also expressed the view that 'law' should include state and territory Acts and delegated legislation. These laws also are subject to accountability requirements. If state and territory laws were not considered law for the purposes of the exception, an organisation, for example, could find that they were subject to conflicting obligations under the *Privacy Act* and a state or territory Act or piece of delegated legislation.

16.31 Professor Dennis Pearce and Stephen Argument state that the usual form of parliamentary oversight is a requirement that delegated legislation be tabled in the parliament.[45] For example, at the Commonwealth level, s 38(1) of the *Legislative Instruments Act 2003* (Cth) requires that all legislative instruments be tabled in each House of Parliament. Pearce and Argument note that the principle that delegated legislation should be reviewed by parliament has been accepted in all Australian jurisdictions, however, in practice such acceptance has been variable.[46]

16.32 In DP 72, the ALRC also expressed the preliminary view that it is unclear whether 'law' should include an order of a court or tribunal; documents that are given the force of law by an Act of Parliament, such as industrial awards; or statutory instruments such as Local Environmental Plans made under planning laws.[47]

16.33 As discussed above, there is some authority for this in the context of privacy law and practice. Further, commentators on the *Australian Constitution*, for example, argue that it is clear that, in the context of case law on s 109 of the *Constitution*, subordinate legislation and awards fall within the term 'law'. Valid subordinate legislation made under a Commonwealth Act will override contrary state legislation.[48]

> Some awards and orders may amount to quasi-judicial determinations that sit uneasily within the rubric of legislation. Nevertheless, the High Court has consistently held

45 D Pearce and S Argument, *Delegated Legislation in Australia* (3rd ed, 2005), 17, 18, 87.

46 Ibid, 17, 18, 87. In Victoria, for example, while s 15 of the *Subordinate Legislation Act 1994* (Vic) requires that a copy of every statutory rule be laid before each House of Parliament within six sitting days of the making of the statutory rule having been notified, s 15 expressly provides that failure to comply with the tabling requirement does not affect the operation or effect of a statutory rule.

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.34].

48 *New South Wales v Commonwealth* (1923) 33 CLR 1, 27, 55, cited in S Ratnapala and others, *Australian Constitutional Law: Commentary and Cases* (2007), 322.

> that a State law is displaced by a valid quasi-judicial decision by force of the Commonwealth Act under which it is made.[49]

16.34 In DP 72, the ALRC also asked whether the definition of 'law' should include common law or equitable duties.[50] The ALRC noted that it is not clear to what extent a 'law' includes a common law or equitable duty for the purposes of the required or authorised exception. The ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC) considered this issue in *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96). The ALRC and AHEC noted that:

> It appears to be accepted that 'law' may include the common law. However, it is not entirely clear whether NPP 2.1(d) permits a doctor to disclose confidential information where the disclosure is covered by the public interest exception to the common law duty of confidentiality. In an Attorney-General's Department information paper, the Government acknowledged that the health profession had a strong respect for the confidentiality of health information and maintained sound privacy practices. The paper stated that the 'legislation is not intended to interfere with those professional values and standards'.[51]

16.35 The ALRC and AHEC concluded that the application of the *Privacy Act* to the disclosure of health information by doctors and other health professionals, in circumstances that may not breach common law or ethical requirements of confidentiality, may require clarification.[52]

16.36 There is some authority, in other legal contexts, for the view that the term 'law' includes the common law. In *Oates v Williams*,[53] the Full Court of the Federal Court held that the phrase 'despite anything in any other law' in a statute under consideration was 'a reference to any law, whether common law or statute'. This statement was later adopted by the High Court in *Attorney-General of the Commonwealth v Oates*.[54]

16.37 Commentators on the *Australian Constitution* argue that, while the term 'law' has an imprecise meaning, the terminology in s 109, when compared with other provisions of the *Australian Constitution*, suggests that the term 'law' in s 109 includes the common law.[55]

---

49 S Ratnapala and others, *Australian Constitutional Law: Commentary and Cases* (2007), 322, discussing *Metal Trades Industry Association v Amalgamated Metal Workers' and Shipwrights Union* (1983) 152 CLR 632, 648–649.

50 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 13–1.

51 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [21.56].

52 Ibid, [21.56].

53 *Oates v Williams* (1998) 84 FCR 348, 353.

54 *Attorney-General of the Commonwealth v Oates* (1999) 198 CLR 162, 169.

55 S Ratnapala and others, *Australian Constitutional Law: Commentary and Cases* (2007), 322. Other provisions of the *Australian Constitution* referred to by way of comparison include ss 76(ii) and 120.

16.38 If the *Privacy Act* is amended to include a definition of 'law', to what extent should common law or equitable duties be captured by that definition? One option is to include a general reference to 'common law and equitable duties'? It may be, however, that the inclusion of such a broad reference has unintended consequences. For example, it is arguable that it could enable an agency or organisation to contract out of its obligations under the *Privacy Act* by way of an exclusion clause. There is no express provision in the *Privacy Act* similar to s 68 of the *Trade Practices Act 1974* (Cth), for example, which renders any term of a contract that seeks to exclude, restrict or modify certain provisions and rights void. It may be that there would be an argument that such a contract would be void or illegal if it infringed public policy.[56]

> A contract may be illegal because it is prohibited by statute, or because it infringes a rule of public policy. It should not, however, be thought that wherever statutory requirements are not fulfilled the resulting contract, if indeed one results, is necessarily illegal or affected by illegality.[57]

16.39 Another option is to refer to particular classes of common law and equitable duties in the definition of 'law'. The question then is which common law and equitable duties should be caught by the definition of 'law'? Three categories of duties could be considered: first, common law or equitable duties of confidentiality; secondly, a school's duty of care; and thirdly, the common law duty of procedural fairness.

16.40 Common law and equitable duties of confidence are discussed in detail in Chapter 15. In essence, legally enforceable obligations to maintain confidence may arise in contract and equity. Duties of confidentiality are owed, for example, by banks;[58] doctors[59] and health professionals;[60] and where information is collected by compulsion under statutory powers.[61] Some duties are subject to exceptions, for example, the banker's duty of confidentiality.[62] As discussed above, the ALRC has previously drawn attention to the need for clarification in relation to duties of confidentiality. Such duties, and the exceptions to those duties, are commonly relied upon in the context of the required or authorised exception.

16.41 Should a school's common law duty of care fall within the definition of 'law'?[63] It is now well established that teachers and school authorities are under a duty to take reasonable care to protect pupils in their charge from a reasonably foreseeable risk of

---

56 ` J Carter and D Harland, *Contract Law in Australia* (3rd ed, 1996), 530.

57 Ibid, 519.

58 *Tournier v National Provincial & Union Bank of England* [1924] 1 KB 461.

59 *Furniss v Fitchett* [1958] NZLR 396.

60 Lawbook Co, *Laws of Australia*, vol 20 Health and Guardianship, [20.7.4] (as at 1 April 2008).

61 *Johns v Australian Securities Commission* (1993) 178 CLR 408, cited in Lawbook Co, *Laws of Australia*, vol 21 Human Rights, [21.4.125] (as at 1 April 2008).

62 *Tournier v National Provincial & Union Bank of England* [1924] 1 KB 461.

63 As noted above, the Appeal Panel of the NSW Administrative Appeals Tribunal (ADT) has held that a school's common law duty to warn falls within the scope of the expression 'any other law' in s 25 of the *Privacy and Personal Information Protection Act 1988* (NSW): *MT v Director General, NSW Department of Education & Training* [2004] NSWADT 194, [83].

injury.[64] The duty includes a positive duty to act[65] and is non-delegable, because of the special relationship between students and school authorities.[66]

16.42 Finally, should the definition of 'law' include common law duties of procedural fairness? There is a duty at common law to afford procedural fairness when exercising a power which affects a person's rights, interests or legitimate expectations.[67] The Privacy Commissioner occasionally has accepted that a disclosure of personal information is necessary to satisfy requirements imposed by the common law principles of procedural fairness.[68]

16.43 In *Skase and Minister for Immigration and Multicultural and Indigenous Affairs*,[69] Deputy President Forgie considered the relationship between s 33 of the *Administrative Appeals Tribunal Act 1975* (Cth) and the IPPs. The issue before the Administrative Appeals Tribunal (AAT) was whether a person, not a party to the application before the AAT, could examine the AAT's file. Deputy President Forgie declined to make an order authorising disclosure under s 33. She noted, however, that s 33 was wide enough to authorise or permit the AAT to make a direction permitting disclosure, referring here to the required or authorised exception in IPP 11.1(d). She commented that issues of procedural fairness would be relevant to the AAT's exercise of discretion in this context.[70] Implicit in Forgie's reasoning is the view that the common law principles of procedural fairness would be caught by the term 'law'.

16.44 In *KD v Registrar, NSW Medical Board*,[71] a case examining the NSW equivalent of the required or authorised by law exception, the Administrative Decisions Tribunal (ADT) found that procedural fairness required the NSW Medical Board to disclose to a medical practitioner an applicant's letter of complaint to the Board concerning the practitioner's conduct of a procedure. As procedural fairness required the Board to disclose the substance of the complaint to the practitioner, the ADT held that the Medical Board could rely on the exception in s 25 of the *Privacy and Personal Information Protection Act 1998* (NSW).[72] The ADT also found, however, that procedural fairness did not require the disclosure of a subsequent letter from the applicant to the Board, enclosing her Medicare claims history.[73]

---

64 R Balkin and J Davis, *Law of Torts* (3rd ed, 2004), 218, [7.2.1], citing *Geyer v Downs* (1977) 138 CLR 91; *Commonwealth v Introvigne* (1982) 150 CLR 258.

65 *Commonwealth v Introvigne* (1982) 150 CLR 258, cited in Lawbook Co, *Laws of Australia*, vol 33 Torts, [33.2.980] (as at 1 April 2008).

66 *Commonwealth v Introvigne* (1982) 150 CLR 258, cited in Lawbook Co, *Laws of Australia*, vol 33 Torts, [33.2.990] (as at 1 April 2008).

67 See, eg, *Kioa v West* (1985) 159 CLR 550; *Haoucher v Minister for Immigration and Ethnic Affairs* (1990) 169 CLR 648; *Annetts v McCann* (1990) 170 CLR 596; *Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564; *Johns v Australian Securities Commission* (1993) 178 CLR 408.

68 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), 41.

69 *Skase and Minister for Immigration and Multicultural and Indigenous Affairs* [2005] AATA 200 .

70 Ibid, [51]–[52].

71 *KD v Registrar, NSW Medical Board* (Unreported, A Britton, 13 January 2004).

72 Ibid, [33]–[41]. The ADT did not specify which limb of s 25 it relied on in reaching this view.

73 Ibid, [39]–[43].

> While the Board has statutory and common law obligations requiring it to provide information to a practitioner the subject of investigation, it does not follow that it is required to disclose all information obtained in the course of that investigation.[74]

16.45 On the other hand, a determination by the Victorian Privacy Commissioner held that, under Victorian legislation, where a person lodges a complaint with an organisation about an individual, arguably it is part of the primary purpose of collection to show the complaint to the individual concerned in the interests of procedural fairness. In any event, the Victorian Privacy Commissioner held that showing the complaint to the individual concerned amounts to disclosure for a related secondary purpose and would be within the complainant's reasonable expectations.[75]

16.46 It is clear that there is authority for the view that certain categories of common law and equitable duties fall within the term 'law' for the purposes of the required or authorised exception.

16.47 The ALRC therefore asked in DP 72 whether the definition of a 'law', for the purposes of determining when an act or practice is required or authorised by or under a law, should include: a common law or equitable duty; an order of a court or tribunal; documents that are given the force of law by an Act of Parliament, such as industrial awards; and statutory instruments such as a Local Environmental Plan made under a planning law.[76]

Submissions and consultations

16.48 The OPC, the Australian Privacy Foundation and a number of other stakeholders supported the inclusion of a non-exhaustive definition of 'law' in the *Privacy Act*.[77]

16.49 Telstra, on the other hand, argued that it was unnecessary to define the term 'law'.

> The term 'laws' is used in this context in many different Acts, and Telstra is not aware of any general principle that the term needs to be defined for the purposes of those Acts, nor is there any great uncertainty caused by this lack of definition. Accordingly, there is no reason why this term should be exhaustively defined in the Privacy Act. Rather, this term should be left to be interpreted in the usual way.[78]

16.50 The OPC argued that, for clarity, any definition of 'law' should remind agencies and organisations that they need to determine, first, whether the particular law applies to them (which may vary depending on the type of entity), and secondly, whether the relevant law in fact requires or authorises the proposed act or practice by that entity.[79] For example, a Commonwealth agency would need to determine whether a state-based statutory instrument applied to it before seeking to relying on its provisions in the context of this exception.

---

74 Ibid, [34], citing Brennan J in *Kioa v West* (1985) 159 CLR 550, 629.
75 *Complainant AG v Local Council* [2007] VPrivCmr 2.
76 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 13–1.
77 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
78 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
79 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

16.51 In terms of what the definition of 'law' should include, there was some support for including an express reference to common law. This support, however, was generally predicated on the need for exceptions to common law duties of confidentiality to be recognised under the *Privacy Act*.[80] The Australian Bankers' Association (ABA) argued that this was an important issue for banks. It noted that a banker's duty of confidentiality in relation to his or her customer is a common law duty to which there are four exceptions under which a bank is authorised or may be required to disclose information:

> (i) with the express or implied consent of the customer; (ii) under compulsion of law; (iii) a duty to the public to disclose; and (iv) the interests of the bank require disclosure.[81]

16.52 The ABA submitted that

> it is important for these exceptions to be recognised under the *Privacy Act* as they currently exist otherwise the duty of confidentiality could be rendered absolute and so in conflict with the permissive aspects of the UPPs placing banks at a significant disadvantage to their competitors.[82]

16.53 The National Catholic Education Commission and Independent Schools Council of Australia questioned whether a school's duty of care towards its pupils is a 'law' for the purposes of the exception.

> Schools apply the current provision as including common law duties such as Schools' common law duty of care towards pupils on the basis that it could not have been intended by the legislature to override this important and frequently litigated duty by privacy legislation.[83]

16.54 The NHMRC submitted that the definition of 'law' should accommodate the need for health care professionals to 'disclose confidential information where the disclosure is covered by the public interest exception to the common law duty of confidentiality'.[84]

16.55 Other stakeholders, however, such as the Public Interest Advocacy Centre (PIAC) and the ATO, thought that including common law and equitable duties in the definition of 'law' would create too much uncertainty.[85] National Legal Aid submitted:

> we foresee problems in extending the definition of required or specifically authorised under law to common law and equitable duties without further qualification. Such

---

80 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

81 Ibid. See also National Australia Bank, *Submission PR 408*, 7 December 2007.

82 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008. What the ABA means by the term 'absolute' is that the duty would not be subject to exceptions.

83 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

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

85 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

> duties are inherently elastic and, if broadly applied, could significantly impact on the protection provided by privacy laws.[86]

16.56 The OPC raised a concern about whether any unintended consequences would arise from specifically including the common law within the scope of 'law'. It noted that common law or equitable principles may lack the 'clarity or certainty of those found elsewhere, such as in legislation'.[87] By way of example, the OPC referred to *Breen v Williams*,[88] in which the High Court held that there was no right of access to medical records under common law. The OPC submitted that it would be concerned if a health service provider sought to rely on the common law principles expressed in *Breen v Williams* as an 'authorisation' to deny access to health information under NPP 2.1(h). The OPC suggested that the ALRC's final Report should explore the extent to which the common law can be relied upon to 'require or authorise' acts.

16.57 In consultations undertaken by the ALRC, concerns were also raised about whether including a broad reference to common law and equitable duties may allow an agency or organisation effectively to contract out of its obligations under the *Privacy Act*. For example, if an organisation was under a contractual obligation to disclose information, it could argue that the obligation for specific performance under that contract is a common law duty which falls within the required or authorised exception.

16.58 There were few submissions which specifically addressed the other proposed limbs of the definition of 'law'. PIAC argued that the definition should only include an order of a court or tribunal to the extent that privacy issues were canvassed in the matter that was before the court or tribunal.[89] PIAC did not support an extension of the definition to statutory instruments (such as Local Environmental Plans) on the basis that they were not subject to parliamentary scrutiny and may be developed by local government without any consideration of privacy issues.[90] The OPC also noted that there was often comparatively little oversight of documents given the force of Commonwealth law, such as industrial awards, but supported the proposal to include industrial awards in the definition.[91]

16.59 The only submission to address the use of the term 'by or under law' in the 'required or authorised' exception in the *Privacy Act*, was that of the OPC, which supported it.[92]

ALRC's view

16.60 There is currently some uncertainty about the scope of the term 'law' in the required or authorised exception. This uncertainty operates on two levels. First, there is uncertainty about the extent to which particular kinds of laws are caught by the term 'law'—for example, whether the term law includes industrial awards given the force of

---

86 National Legal Aid, *Submission PR 521,* 21 December 2007.
87 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
88 *Breen v Williams* (1996) 186 CLR 71.
89 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.
90 Ibid.
91 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
92 Ibid.

Commonwealth law. Secondly, there is uncertainty stemming from apparent inconsistencies in the interpretation of whether particular categories of laws are caught by the term 'law' in the context of the IPPs, as opposed to the NPPs. For example, as noted above, the OPC's *Guidelines to the National Privacy Principles* provide that 'law' includes common law,[93] however, its *Plain English Guidelines to the Information Privacy Principles* indicate that, for agencies, 'law' generally does not include common law.[94]

16.61 The ALRC acknowledges the view of Telstra that it is not necessary to define the term 'law' in the *Privacy Act*. The ALRC notes, however, that the term 'law' is currently defined in several Commonwealth statutes,[95] although not as comprehensively as that proposed in DP 72.

16.62 It is important to articulate clearly the scope of the required or authorised exception, which is included in six of the model UPPs. Expressly setting out categories of law in an inclusive definition should generate more clarity and certainty in the application of the exception.

16.63 The definition of 'law' for the purposes of the 'required or authorised' by law exception should include Commonwealth and state and territory Acts and delegated legislation. In DP 72, the ALRC proposed including statutory instruments, such as a Local Environmental Plan made under a planning law in the definition. The ALRC acknowledges, however, the argument made in PIAC's submission that such instruments may not be subject to the same level of parliamentary oversight as Acts and pieces of delegated legislation. Accordingly, the ALRC recommends that the definition refer only to delegated legislation, so as to ensure that those legislative instruments captured by the definition are subject to some form of parliamentary review. In the ALRC's view, a reference to statutory instruments (such as Local Environmental Plans) should not be included.

16.64 The ALRC accepts the concerns raised by stakeholders that including a broad reference to 'common law and equitable duties' in the definition of 'law' may have unintended consequences. It may enable, for example, an agency or organisation to contract out of its obligations under the *Privacy Act* by way of an exclusion clause. For this reason, rather than referring to 'common law and equitable duties' generally in the definition of law, it is preferable to specify particular common law and equitable duties.

16.65 A number of stakeholders supported the inclusion of common law and equitable duties of confidentiality and the exceptions to those duties, in the definition of 'law'. The ALRC has previously highlighted the need for greater clarity in this area.[96] In the

---

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

94 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), 41.

95 See, eg, *Evidence Act 1995* (Cth) s 3, Dictionary: cl 9, Part 2; *Fringe Benefits Tax Assessment Act 1986* (Cth) s 136(1); *Human Rights and Equal Opportunity Act 1986* (Cth) s 3(1).

96 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [21.56].

ALRC's view, common law and equitable duties of confidentiality should be included in the definition of 'law'. This definition should make express mention of the exceptions to such duties.

16.66 One stakeholder argued that it was important that a school's duty of care was reflected in the definition of 'law'.[97] As noted above, there is some authority for the view that a school's duty of care will fall within the term 'law'. Given the limited authority on point, however, the ALRC is not convinced that a specific reference to a school's duty of care in the definition of 'law' is warranted. In reaching this conclusion, the ALRC is not expressing the view that a school's common law duty of care will never fall within the definition of the term 'law' for the purposes of the required or authorised exception. Whether it does or does not will depend on the factual circumstances of a particular case.

16.67 There is some support for the view that 'law' in the context of the required or authorised exception should include the common law principles of procedural fairness. No submissions specifically addressed the issue, however, and the ALRC's view is that no specific reference should be made to common law principles of procedural fairness in the definition of 'law'. As with a school's duty of care, a strong consideration in reaching this view is that the definition of law recommended by the ALRC is inclusive. In reaching this conclusion, the ALRC is not expressing the view that the common law principles of procedural fairness will never be caught by the term 'law' for the purposes of the required or authorised exception.

16.68 If confusion develops as to the extent to which common law or equitable duties other than duties of confidentiality fall within the definition of 'law', it may be appropriate for the OPC to issue guidance in this regard.

16.69 The ALRC proposed in DP 72 that the definition of a 'law' should include an order of a court or tribunal. The few submissions which addressed this issue did not provide any compelling arguments for its omission. The ALRC remains of the view that orders of a court or tribunal should be included in this definition.

16.70 The ALRC also proposed in DP 72 that the definition should include documents given the force of law by an Act of Parliament, such as industrial awards. The OPC supported this proposal, although it noted that there can be comparatively little oversight of such documents. The ALRC notes that such documents have been interpreted as constituting laws for the purposes of s 109 of the *Australian Constitution*. For these reasons, the ALRC confirms its view that this limb should be included in the definition of 'law'.

16.71 Finally, the phrase 'by or under law' should be retained. There is judicial authority to support the view that the terms 'by' and 'under' have slightly different meanings. No concerns about the phrase were raised in submissions and the OPC supported its retention.

---

97 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

Recommendation 16–1 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:

(a) Commonwealth, state and territory Acts and delegated legislation;

(b) a duty of confidentiality under common law or equity (including any exceptions to such a duty);

(c) an order of a court or tribunal; and

(d) documents that are given the force of law by an Act, such as industrial awards.

'Specifically authorised'

16.72 While acts and practices that are 'required' by law will be relatively rare, the 'authorised' by or under law exception could potentially except a wide range of acts and practices from the limits imposed by the *Privacy Act*. One issue for consideration is whether the 'authorised' by or under law exception should be narrowed. The European Union Article 29 Data Protection Working Party has criticised the required or authorised exception under the *Privacy Act* as being imprecise:

> The wording 'authorised' as opposed to 'specifically authorised' which existed in the January 1999 edition of the National Principles can also be read to mean that all secondary purposes that are not forbidden are allowed. In the working party's view such a wide exemption would virtually devoid the purpose limitation principle of any value.[98]

16.73 The term 'specifically authorised' is used in a number of federal Acts. Section 51 of the *Trade Practices Act 1974* (Cth) provides that, in deciding whether a person has contravened Part IV of the Act (restrictive trade practices), anything specified in, or 'specifically authorised' by certain laws must be disregarded. Section 43A of the *Environment Protection and Biodiversity Conservation Act 1999* (Cth) (EPBC Act) refers to 'specific environmental authorisation'. The Federal Court considered the meaning of this phrase in *Minister for the Environment & Heritage v Greentree (No 2),*[99] in which Sackville J considered whether the respondents were specifically authorised to undertake certain activities on land that was 'declared Ramsar wetland'.

> The language of s 43A(1)(b) of the EPBC Act implies that there is a distinction between an action which is authorised under an Act and one which is specifically authorised … in my view [specifically authorised] does not mean that the authorisation must only relate to a single site or to a single activity on land. It is in my

98 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.

99 *Minister for the Environment & Heritage v Greentree (No 2)* [2004] FCA 741.

> view enough that the authorisation covers a defined class of activities or identifiable land which includes the subject land.[100]

16.74 In DP 72, the ALRC noted that the required or authorised exception is essential to grant governments the discretion to provide that personal information be handled in particular ways. The ALRC therefore proposed that it remain as an exception to a number of the proposed UPPs. The ALRC proposed, however, that a new exception be provided in relation to certain principles—namely, an exception where an act or practice is 'specifically authorised'. The ALRC expressed the preliminary view that an exception for acts and practices that are 'specifically authorised' would require the law expressly to authorise a defined class of acts and practices that would otherwise contravene the principle in the *Privacy Act*. Accordingly, it would require the Australian Parliament and state and territory parliaments to turn their minds to how the proposed law would interact with the *Privacy Act*, and the competing interests for and against the handling of personal information in a particular manner.[101]

16.75 The ALRC proposed including the 'specifically authorised' exception in the proposed 'Collection' and 'Specific Notification' principles.[102] NPP 10.1(b) currently provides that an organisation must not collect sensitive information about an individual unless the collection is required by law. In DP 72, the ALRC expressed the view that this exception is too narrow. The ALRC considered proposing an exception to the 'Collection' principle if an act or practice were 'authorised by law', but reached the preliminary view that such an exception may be too wide, as it could include laws that impliedly authorise certain acts and practices. The ALRC proposed, therefore, that an agency or organisation should not collect sensitive information unless the collection is 'required or specifically authorised by or under law'.[103]

16.76 The ALRC also proposed the introduction of a new 'Specific Notification' principle that would require agencies and organisations to take reasonable steps to inform an individual of certain matters. The ALRC proposed, however, that agencies should not be required to take reasonable steps to inform individuals of the matters listed in the proposed principles if they were required or specifically authorised by or under law not to do so.[104] As discussed in Chapter 23, however, the ALRC no longer holds the view that this exception is appropriate.

16.77 In DP 72, the ALRC also asked whether the proposed 'Use and Disclosure' principle should contain an exception allowing an agency or organisation to use or disclose personal information for a purpose other than the primary purpose of

---

100 Ibid, [153].

101 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.47].

102 The name of the 'Specific Notification' principle has now changed to the 'Notification' principle: see Ch 23.

103 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 19–2.

104 See Ibid, Ch 20.

collection where this is 'required or specifically authorised by or under law,' instead of simply 'required or authorised by or under law'.[105]

Submissions and consultations

16.78 Few submissions addressed the question of whether the term 'specifically authorised' should be adopted in favour of the term 'authorised' in all of the UPPs. Those that did comment supported the inclusion of the term 'specifically authorised' so as to 'promote regulatory certainty'.[106] For example, the OPC stated:

> As the Office understands it, the effect of including the term 'specifically authorised', as opposed to simply 'authorised', is that the relevant principle will only permit information-handling acts or practices that are expressly authorised by or under law. Such an amendment would lessen regulatory complexity and uncertainty by clarifying that legal authorities for various acts or practices cannot be implied or incidental.[107]

16.79 This view was shared by Privacy NSW.[108] Many stakeholders, however, raised concerns about the use of the term 'specifically authorised' in the 'Use and Disclosure' principle and the 'Collection' principle. Whilst the case for the inclusion of this term will be considered in Chapters 25 and 21 respectively, mention is made here of the submissions which raised concerns with general application.

16.80 A number of government agencies[109] expressed concern about the proposed extension of the exception in the context of the 'Use and Disclosure' principle.[110] The ATO argued that the proposed approach does not 'adequately take into account the nature of much Commonwealth law on disclosure'.[111] It submitted that the ATO currently relied on implied authorisations in some contexts, 'for example, laws may lay down a specific scheme of which some uses and disclosures of personal information are an inseparable part'.[112] It noted that many taxation law provisions were of this nature.[113]

> Also, there are important provisions in taxation law which evidence a parliamentary intention that disclosures of taxation information are made for defined aims, but where it could be said that disclosures are not 'specifically' authorised as the content of potential disclosures is not specified. While disclosures made under these provisions are clearly 'authorised by law', it is possible that some would not be able to be said to be '*specifically* authorised by law' …

---

105 Ibid, Question 22–1. The ALRC also proposed the use of the term in the range of defences to the proposed statutory cause of action for invasion of privacy: Ibid, Proposal 5–5. The ALRC no longer recommends the use of this term in this context: see Ch 74.

106 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; Privacy NSW, *Submission PR 468*, 14 December 2007.

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

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

109 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

110 This is discussed in detail in Ch 22.

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

112 Ibid.

113 Ibid.

> We expect that many existing Commonwealth laws would contain disclosure powers of this type, and that a *Privacy Act* requirement that disclosures be specifically authorised could compromise disclosures which Parliament clearly intended could be made.[114]

16.81 The Australian Federal Police also objected to the use of the word 'specifically'.

> The use of the word '*specifically*' assumes that all the powers and functions of an agency will always be set out expressly in the legislation. However, practical experience demonstrates that the legislation does not always address every issue and it is sometimes necessary to determine what is required by necessary implication as well as by what is expressed. There is a real concern that the inclusion of the word '*specifically*' would only enable an agency and the courts to look at specific powers.[115]

16.82 This view was also shared by Medicare Australia:

> We do not agree that the requirement be narrowed to a condition where the use or disclosure be 'specifically' authorised. This would necessitate that legislation governing the functions and activities of an agency would need to cover all foreseeable actions in administering the programs the agency is responsible for, and for either anticipating future developments or regularly amending existing legislation to keep up with changes. In the case of Medicare Australia, we have specific functions expressed in legislation, but the activities required to administer those functions are not always specifically defined.[116]

16.83 This lack of support extended to organisations.[117] For example, Avant Mutual Group Ltd argued that adding the term 'specifically authorised' was superfluous. It noted that there are many laws which are not prescriptive and argued that the introduction of the term 'specifically' could have the 'unintended consequence of preventing the release of personal information when a fair reading of the law allows disclosure', citing s 40(3) of the *Insurance Contracts Act 1984* (Cth) as an example.[118]

16.84 This view was shared by Telstra, which argued that the amendment was unnecessary and only would create uncertainty. Telstra argued that a use or disclosure was either 'authorised or not authorised by or under law'.[119] The Australian Finance Conference expressed concern about the 'potential additional compliance obligations that such a narrowing could attract', which, in its view, could impose major operational costs.[120]

---

114 Ibid.
115 Australian Federal Police, *Submission PR 545*, 24 December 2007.
116 Medicare Australia, *Submission PR 534*, 21 December 2007.
117 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; National Australia Bank, *Submission PR 408*, 7 December 2007.
118 Avant Mutual Group Ltd, *Submission PR 421*, 7 December 2007.
119 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.
120 Australian Finance Conference, *Submission PR 398*, 7 December 2007.

16.85 Similar concerns were expressed in submissions concerning the use of the term 'specifically authorised' in relation to the collection of sensitive information.[121] For example, the Australian Communications and Media Authority submitted:

> This Proposal has potentially far reaching implications and may impact on the capacity of agencies to fulfil their statutory functions and powers … A 'specific authorisation' to 'collect' criminal record information will frequently not exist and it is usually the case that an agency will have this authority by implication.[122]

ALRC's view

16.86 Legislation should set out clearly whether it is intended to require or authorise an act or practice for the purposes of the *Privacy Act.* In the interest of clarity and transparency, such provisions should set out the type of information to be included, the scope of the requirement or authorisation, and the extent to which the *Privacy Act* applies to the handling of that information.

16.87 It is the ALRC's view, however, that the term 'specifically authorised' should not be adopted in the *Privacy Act.* While there is little case law on 'authorised by law', that which does exist demonstrates that authorisation involves permission and, so, more than an absence of prohibition.[123] Even where disclosure is 'authorised', courts will set limits on the extent of disclosure.[124]

16.88 While the inclusion of the phrase 'specifically authorised' was supported by a number of stakeholders, strong concerns were expressed by agencies. Agencies argued that it would have far-reaching implications, affecting their ability to fulfil their statutory functions and exercise their powers. Agencies may need to rely on implied authorisations, but arguably would be prevented from doing so if the term 'specifically authorised' were included in the *Privacy Act*.

16.89 In Chapter 27, the ALRC recommends that the *Privacy Act* be amended to empower the Privacy Commissioner to direct an agency to provide to the Privacy Commissioner a Privacy Impact Assessment (PIA) in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[125] In the ALRC's view, a PIA generally should be prepared when a provision in new legislation may require or authorise an act or practice relating to the handling of personal information that would otherwise be regulated by the *Privacy Act*.[126] If a PIA is prepared, federal Parliament will be required to turn its mind to how the proposed law will interact with the *Privacy Act* and assess the competing interests for and against the handling of personal information in a particular manner.

---

121 Australian Federal Police, *Submission PR 545*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007. This is discussed in detail in Ch 19.

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

123 See, eg, *Caratti v Federal Commissioner of Taxation (Cth)* (1999) 99 ATC 5044, [27].

124 *Fletcher v EEBME Pty Ltd* (2007) 213 FLR 1, [31].

125 Rec 47–4.

126 See Ch 47.

Clear references to an exception in legislation

16.90 Federal legislation contains a number of provisions that require or authorise certain acts or practices for the purpose of the *Privacy Act*. Most of these provisions relate to the disclosure of personal information.[127] For example, s 42(1)(g) of the *Australian Passports Act 2005* (Cth) provides that the minister performing functions under the Act may request certain persons to disclose personal information about a person to whom an Australian travel document has been issued. Section 42(3) then provides that, for the purposes of IPP 11(1)(d) and NPP 2.1(g), such a disclosure is required or authorised by law.

16.91 The interaction between these provisions and the *Privacy Act*, however, is not always clear. For example, some provisions under federal legislation require or authorise disclosure of information, but do not state that it is required or authorised for the purposes of the *Privacy Act*.[128] Other provisions, such as s 488B of the *Migration Act 1958* (Cth), provide that certain disclosures of information may occur 'even if the information is personal information (as defined in the *Privacy Act 1988*)'.[129]

16.92 In DP 72, the ALRC noted that stakeholders had submitted that legislation which intends to rely on the required or authorised exception should include clear references to this fact in the legislation.[130] It was noted that ambiguity in legislation can cause uncertainty for agencies, individuals, organisations and, potentially, the OPC, as to how information should be handled, and whether relevant provisions meet the requirements under the *Privacy Act*.[131] Amending legislation which is intended to rely on the required or authorised exception so that it includes clear reference to this in the legislation is one option that was considered.[132]

ALRC's view

16.93 It would be too onerous to amend all existing federal, state and territory legislation that may require or authorise an act or practice relating to the handling of personal information. Federal, state and territory parliaments should, however, ensure that proposed laws that are intended to rely on the required or authorised exception should, where possible, make such authorisation express. Ideally, the legislation also should include clear references to the exception under the *Privacy Act*.

---

127 See, eg, *Australian Passports Act 2005* (Cth) s 42; *Building and Construction Industry Improvement Act 2005* (Cth) s 65; *Military Rehabilitation and Compensation Act 2004* (Cth) s 409; *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 3A; *Telecommunications Act 1997* (Cth) s 303B; *Wheat Marketing Act 1989* (Cth) s 59; *Veterans' Entitlements Act 1986* (Cth) s 38AA; *Migration Act 1958* (Cth) ss 321, 336FB.

128 See, eg, *Snowy Hydro Corporatisation Act 1997* (Cth) s 56; *Wheat Marketing Act 1989* (Cth) s 59.

129 See also *Customs Act 1901* (Cth) ss 64ACA, 64ACB, 64AF, 273GAB.

130 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

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

132 Ibid; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

Review of legislation

16.94 In submissions to this Inquiry the Office of the Information Commissioner Northern Territory and the OVPC submitted that legislation that predates the *Privacy Act* may continue to justify what would otherwise constitute breaches of privacy principles. The importance of requiring any legislation that raises privacy issues to be reviewed at appropriate intervals to confirm that the Parliament continues to accept that it reflects an appropriate balance between privacy interests and other interests was emphasised in both submissions.[133]

16.95 The Privacy Commissioner currently has various powers to review legislation for these purposes. These powers include a power under s 27(1)(f) of the *Privacy Act* to provide, on request or on the Commissioner's own initiative, advice to a minister, agency or organisation on any matter relevant to the operation of the Act. In the ALRC's view, this power enables the Privacy Commissioner to monitor legislation that requires or authorises certain acts and practices for the purposes of the *Privacy Act*, and provide advice to the minister responsible for that legislation, if those acts and practices are no longer considered appropriate. The Privacy Commissioner should exercise his or her power under this provision where appropriate.

A list of laws that require or authorise acts and practices

16.96 One option raised by the OPC in response to the Issues Paper, *Review of Privacy* (IP 31), is the compilation of a list of provisions that require or authorise acts or practices that would otherwise be regulated by the *Privacy Act*. Such a list would provide clarity for agencies, organisations, individual consumers and privacy regulators about whether certain laws met the criteria of the exception. The OPC suggested that such a project may require the coordination of numerous agencies and organisations, such as the OPC and, possibly, the Australian Government Attorney-General's Department (AGD).

16.97 The OPC suggested that the list could act as a centralised resource for drafting and, potentially, the development of a standardised provision. The list also could serve an educative function by prompting agencies to consider privacy implications when developing legislation.[134]

16.98 In DP 72, the ALRC noted that this proposal raised a range of issues. A threshold question is whether the list should have the force of law. One option is to locate the list in a schedule to the *Privacy Act*, another is to promulgate it in regulations. A less formal method is for the list to published by the AGD or the OPC, this would enable the content of the list to be amended more readily, but would not have the same legal authority as, for example, a schedule to the *Privacy Act*.

---

133 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007. See also Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

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

16.99 A further issue is whether the list should be comprehensive or indicative. One concern is that the practice of identifying some provisions and not others could produce an interpretation that listing was a necessary precondition for the exception to operate.

16.100 Another issue for consideration is which agency should be responsible for the preparation of such a list. One option would be for the OPC to compile. It is questionable, however, whether the OPC would have the resources to undertake such a task. Another option would be for the AGD to compile the list. Agency heads could supply the AGD with a list of provisions in legislation they administer that require or authorise the handling of personal information.

16.101 In DP 72, the ALRC asked whether a list should be compiled of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*. The ALRC also asked whether such a list should have the force of law, whether it should be comprehensive or indicative and what body should be responsible for compiling and updating the list.[135]

Submissions and consultations

16.102 There was a range of views concerning this proposal. Some stakeholders expressed support for a comprehensive list;[136] and some supported a list which had the force of law.[137] For example, GE Money expressed the view that a list that was not comprehensive, or that did not have the force of law, would not provide certainty and may in fact cause further confusion.[138] PIAC argued that:

> compilation and maintenance of a comprehensive list of laws that require or authorise acts or practices that would otherwise be regulated by the *Privacy Act* would provide greater clarity.[139]

16.103 PIAC also argued that compiling the list would provide a useful opportunity to review such laws to ensure they are consistent with recommended amendments to the *Privacy Act*.

16.104 The majority of stakeholders, however, argued that, if a list were to be developed, it should be indicative.[140] The ABA argued that omission from the list should not mean that a particular law cannot be relied upon to satisfy the exemption.[141]

---

135 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Question 13–2.

136 Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; GE Money Australia, *Submission PR 537,* 21 December 2007; National Health and Medical Research Council, *Submission PR 397,* 7 December 2007.

137 GE Money Australia, *Submission PR 537,* 21 December 2007; National Legal Aid, *Submission PR 521,* 21 December 2007.

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

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

140 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 Taxation Office, *Submission PR 515,* 21 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; National Australia Bank, *Submission PR 408,* 7 December 2007.

141 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008.

The Australian Privacy Foundation supported an indicative list, on the basis that it was impracticable to compile and maintain an exhaustive list.[142]

16.105 Some stakeholders suggested that the list should be maintained by the OPC.[143] The NHMRC submitted that it should be maintained by the AGD.[144]

16.106 Other stakeholders, notably the OPC, disputed the merits of maintaining such a list at all. While acknowledging that it proposed the development of a consolidated digest of all relevant legislative provisions, the OPC stated that, upon further reflection, it was not convinced of the merits of the proposal.

> In particular, the Office believes that the likely benefits of such a digest of laws may not justify the resources required to develop and maintain it. Accordingly, the Office would not seek to have primary responsibility for such a digest if it were adopted.[145]

16.107 The OVPC shared the view that the compilation of a list would be impractical.[146] A number of stakeholders—even some that supported the development of a comprehensive list—acknowledged that the compilation and continued updating of such a list would require significant resources.[147] Others noted that the expenditure of public resources for this purpose was not warranted.[148]

16.108 The Government of South Australia pointed out that it was already lawful for the OPC to publish educational material about principles, which could offer examples of disclosures authorised by law.[149]

ALRC's view

16.109 The benefits of creating a comprehensive or binding digest of relevant laws are unlikely to justify the resources required to develop and maintain it. The OPC already provides examples of particular statutes which require the use or disclosure of information in the context of NPP 2.1(g).[150] Providing a list of examples of legislation would assist in providing greater clarity and facilitating compliance. The ALRC agrees that it should be made clear that omission from the list does not mean that a particular law cannot be relied upon for the purpose of the required or authorised by or under law exception.

---

142 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
143 Ibid; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
144 National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
145 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
146 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. See also Australian Taxation Office, *Submission PR 515*, 21 December 2007.
147 GE Money Australia, *Submission PR 537*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
148 Government of South Australia, *Submission PR 565*, 29 January 2008; Queensland Government, *Submission PR 490*, 19 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.
149 Government of South Australia, *Submission PR 565*, 29 January 2008.
150 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001), 2 (NPP 2.1(g)).

Recommendation 16–2 The Office of the Privacy Commissioner should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. This guidance should include:

(a) a list of examples of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*; and

(b) a note to the effect that the list is intended to be a guide only and that omission from the list does not mean that a particular law cannot be relied upon for the purposes of a 'required or authorised by or under law' exception in the model Unified Privacy Principles.

Census and Statistics Act 1905 (Cth)

16.110 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).[151] The census is regarded as the most important source of statistical information in Australia. The *Privacy Act* applies the IPPs to personal information collected as part of the census.[152] The *Census and Statistics Act* also contains a number of provisions, including secrecy provisions, directed to protecting information collected as part of the census.[153]

16.111 Before the 2001 Census, all name-identified information from past censuses was destroyed on completion of statistical processing.[154] In 2000, the Australian Government introduced legislation that provided for the retention of census data.[155] This legislation was put in place for the 2001 Census on a trial basis. The *Census Information Legislation Amendment Act 2006* (Cth) amended the *Census and Statistics Act* to ensure that, subject to the household's consent, name-identified information collected in the 2006 Census, and all subsequent censuses would be stored by the National Archives of Australia (National Archives) in order to preserve it for release for research after a closed access period of 99 years.[156]

---

151 *Census and Statistics Act 1905* (Cth) s 8.

152 Under the *Privacy Act*, personal information collected by the ABS for a census is collected for a lawful purpose directly related to a function or activity of the ABS and is necessary and directly related to that purpose: *Privacy Act 1988* (Cth) s 14, IPP 1.1.

153 *Census and Statistics Act 1905* (Cth) ss 7, 8A, 13, 19, 19A, and 19B. For example, s 19A provides that the Australian Statistician or an ABS officer must not at any time, during the period of 99 years from the day for a census, divulge or be required to divulge information contained in a census form to an agency, a court or a tribunal.

154 Explanatory Memorandum, Census Information Legislation Amendment Bill 2000 (Cth), 2.

155 *Census Information Legislation Amendment Act 2000* (Cth).

156 Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth), 2. In 2001, 52% of Australians gave consent to have their name-identified information released after 99 years. For 2006, the participation rate was 56.1%: Australian Bureau of Statistics, 'Retention Facts and Figures (the Census Time Capsule)' (Press Release, 27 June 2007).

16.112 Another recent development is the Census Data Enhancement (CDE) project, the primary objective of which is to enhance the value of the census by combining it with future census data and, possibly, other datasets held by the ABS.[157] The central feature of this project would have been the Statistical Longitudinal Census Dataset (SLCD), involving all respondents to any census. Due to privacy concerns raised in submissions to the Senate Legal and Constitutional References Committee,[158] and a PIA[159]—for example, the risk that in the future such a rich dataset may be used for administrative and other non-statistical uses—the CDE proposal was substantially modified.[160] The SLCD will now be based on a 5% sample of the population, which in the ABS's view, will make it unsuitable for such other uses.[161]

16.113 The ALRC considered in DP 72 whether personal information collected pursuant to the *Census and Statistics Act* was protected adequately.[162] While the ABS submitted that protection was adequate,[163] other stakeholders noted concerns held by some individuals in the community—for example, relating to the amount of detail collected for household surveys and whether some of the questions in the census are unnecessarily intrusive.[164] The need for confidentiality was linked to the public interest in truthful, and therefore reliable, census responses.[165]

16.114 In DP 72, the ALRC did not make a proposal in relation to the *Census and Statistics Act*. The OPC submitted in response to DP 72, however, that in conducting future population and housing censuses, the ABS should consider whether greater emphasis should, or could, be placed on explaining administrative and other measures that protect privacy and which address the specific types of concerns raised by the community with the OPC.[166]

ALRC's view

16.115 The ALRC does not make a recommendation in relation to the operation and administration of the *Census and Statistics Act*. The information contained in name-

157 Australian Bureau of Statistics, *2006 Census: Census Data Enhancement* <www.abs.gov.au> at 6 May 2008. A Discussion Paper on the project was released in April 2005: Australian Bureau of Statistics, *Enhancing the Population Census: Developing a Longitudinal View* (2005).

158 See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.113]–[5.116].

159 Pacific Privacy Consulting, *Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics* (2005).

160 Australian Bureau of Statistics, 'ABS Develops a New View of Records Across Successive Censuses' (Press Release, 18 August 2005).

161 See Australian Bureau of Statistics, 'Methodological News: Summary—Updates on the Census Data Enhancement Project' (Press Release, 18 December 2007).

162 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.50]–[13.58]. See also Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(i).

163 Australian Bureau of Statistics, *Submission PR 96*, 15 January 2007.

164 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Saving Our Census and Preserving Our History* (1998), [4.10]–[4.14].

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

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

identified census records is a valuable source for historians, historical sociologists and other researchers; and is protected adequately under the current regime.[167]

16.116 The ALRC notes that the collection and retention of name-identified information only is to occur with the consent of the individual.[168] This is consistent with the current IPPs and the model UPPs. Further, the sensitivity of much personal information has diminished after 99 years. The legislated closed period of 99 years is a recognition of this fact.

16.117 The retention of records by the National Archives for a period of 99 years is consistent with IPP 4 (Storage and Security of Personal Information) and UPP 8 (Data Security). The protection provided by the *Archives Act 1983* (Cth) is robust and beyond that accorded to other personal information.[169] During the time it is in the closed period, the retained name-identified information is expressly excluded from provisions for special access under s 56 of the *Archives Act* or by disclosure by National Archives staff, including to a court or tribunal.[170]

16.118 In relation to the SLCD, the ALRC acknowledges the serious concerns about the privacy risks associated with the development of a rich longitudinal dataset that relates to the entire Australian population. The ALRC notes the concerns of stakeholders that such a dataset might be too attractive for future non-statistical or administrative uses. The ALRC agrees with the ABS that the modified proposal for the SLCD to be based on a 5% sample of the population, augmented at each census with a further 5% sample of people who have been born in, or migrated to, Australia since the preceding census, will minimise the usefulness of the dataset much less attractive for other uses, including administrative and other non-statistical uses.

16.119 The ALRC acknowledges the privacy concerns that some members of the public have about the census. The ALRC is satisfied that the legislative framework within which the ABS operates and conducts the census adequately protects personal information. The ABS is subject to the *Privacy Act* as well as confidentiality provisions under the *Census and Statistics Act*. Names and addresses are not retained for longer than the period required for census processing, and are used only in relation to census processing and for ABS quality studies. Names and addresses are destroyed at the end of census processing.[171]

16.120 Further, various administrative arrangements for the collection of census data are designed to protect the privacy of individuals participating in the census. For example, householders who do not wish other members of the household to see their information, may request a personal census form. Those who are concerned about the

---

167 In the late 1970s, the ALRC conducted an inquiry into privacy issues and the census: Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979), x–xvi. A number of these recommendations have been implemented. See, eg, *Census Information Legislation Amendment Act 2000* (Cth).

168 *Census and Statistics Act 1905* (Cth) s 8A.

169 National Archives of Australia, *Submission PR 199*, 20 February 2007.

170 *Archives Act 1983* (Cth) ss 22B, 30A.

171 D Trewin (Australian Statistician), 'Census Data Enhancement Project—Statement of Intention' (Press Release, 18 August 2005).

census collector seeing the form can ask for a privacy envelope or can complete the census form online. Householders who still have concerns can ask the census collector for a reply-paid 'mailback' envelope to post their completed form directly to the ABS.[172]

16.121 The ALRC agrees with the OPC's view, however, that the ABS may alleviate public concern about perceived privacy issues associated with the use of census data by placing greater emphasis on explaining administrative and other measures that protect privacy when conducting future population and housing censuses.

Corporations Act 2001 (Cth)

16.122 Section 168 of the *Corporations Act* requires companies and registered schemes to maintain a register of members and, if relevant, a register of option holders and a register of debenture holders. Section 169 of the Act requires a register of members to contain certain details, including the member's name and address, the date on which the member's name was entered on the register, as well as other details, such as the shares held by each member.

16.123 Under ss 173 and 174 of the *Corporations Act*, companies, registered schemes and persons who maintain registers on behalf of companies and registered schemes must allow anyone to inspect these registers. These sections are examples of provisions that require or authorise the disclosure of information for the purposes of the *Privacy Act*. It is unlikely, therefore, that compliance with the *Corporations Act* requirements would breach NPP 2.

16.124 Section 177 of the *Corporations Act* provides that it is a criminal offence to use information about a person obtained from a register to contact or send material to the person, or to disclose information obtained from a register knowing that the information is likely to be used to contact or send material to the person. An exception to that rule is where the use of the information is connected with the membership, or approved by the company.[173]

16.125 Link Market Service submitted that the provisions relating to access to registers under the *Corporations Act* are contrary to the NPPs.[174] It noted that, under the *Privacy Act*, a company that maintains a members' register cannot provide personal information except for the primary purpose of managing a members' register, and yet under the *Corporations Act* it is able to disclose information that would not usually be disclosed.

> Practically we cannot, for example, disclose information to a shareholder that calls in without providing their unique identifier (their Securityholder Reference Number) but

172 Australian Bureau of Statistics, *2006 Census: Privacy and Confidentiality* <www.abs.gov.au> at 6 May 2008.

173 *Corporations Act 2001* (Cth) s 177(1A).

174 Link Market Service, *Submission PR 2*, 24 February 2006.

> can allow access to a register to a member of [the] public if they visit our offices to a view a register (in this process they can see a specific individual's holding balance).[175]

16.126 In *IMF (Australia) Ltd v Sons Of Gwalia Ltd*,[176] however, French J made the following comment about the relationship between s 177 of the *Corporations Act* and the *Privacy Act*:

> Section 177 is designed to protect the privacy of shareholders by limiting the use to which information about them may be put. By way of example, which is given in a note to the section, the use of information on the register for the direct marketing of goods or services, would fall within the prohibition. The prohibition in s 177 is consistent with the National Privacy Principles set out in Schedule 3 of the *Privacy Act 1988* (Cth).
>
> It appears reasonably clear from its terms that the purpose of s 177 is to protect the privacy of shareholders by limiting permitted uses of information obtained from the register about them. The section would not permit the use of information on the register for direct marketing to shareholders of goods and services unrelated to their status as shareholders and it may be the case that even company approval of the use of information on the register will be constrained by the National Privacy Principles to which reference has already been made.[177]

16.127 Particular concerns have also been raised about the personal information held by mutual entities, such as credit unions. It has been argued that the personal information on a credit union's member register is more detailed and revealing than information on an ordinary company register,[178] and that access to this information will encourage misuse of this information.[179] Amendments have been made to the *Corporations Regulations 2001* (Cth) to deal with this issue.[180] Regulation 12.8.06 of the *Corporations Regulations* allows mutual entities to:

- have a separate register of 'member shares' being the shares which are issued by them to their customers;
- require the party seeking access to agree in writing that the information about members which is gained will be divulged only to certain named persons and used only for certain specified purposes; and
- refuse access if it is not satisfied that access is being sought by a member who intends to call a meeting of members, or for another purpose approved by the Australian Securities and Investments Commission (ASIC).

16.128 Further, the *Corporations Amendment Regulations 2007 (No 9)* (Cth) provide that when a person seeks access to a register of members of certain body corporates (a

---

175 Ibid.

176 *IMF (Australia) Ltd v Sons Of Gwalia Ltd (Administrator Appointed) ACN 008 994 287* (2004) 211 ALR 231.

177 Ibid, [52]–[53].

178 See Information Integrity Solutions, *Customer Lists: Background Paper for CUSCAL Industry Association* (2005).

179 Credit Union Industry Association and others, *Issues Overview: Member Registers, Takeovers and Mutuals* (2006).

180 *Corporations Amendment Regulations 2003* (Cth).

credit union, credit society and building society) and the person has given a statutory declaration in relation to the use of that information and paid the reasonable costs of contacting the members, or sending material to the members, the body corporate must do everything that is reasonably possible to arrange for the members to be contacted, or for the material to be sent to the members, on the person's behalf by a third party service provider nominated by the body corporate.[181]

16.129 In IP 31, the ALRC asked whether it was appropriate that the disclosure of a shareholder's personal details in a register of members, register of debenture holders or a register of option holders under the *Corporations Act* is a disclosure of personal information that is permitted for the purposes of NPP 2.[182] Stakeholders' views were canvassed in detail in DP 72.[183] The ALRC reached the preliminary view that the *Corporations Act* provides significant protection of personal information held on a register and that the current level of protection strikes an appropriate balance between the competing interests at play. The ALRC also noted that the member registers of mutuals, such as credit unions, receive extra protection under the *Corporations Regulations*. Accordingly, the ALRC did not make a proposal in relation to the *Corporations Act* in DP 72.

Submissions and consultations

16.130 Only two submissions were received on this issue in response to DP 72. The OPC noted that the handling of personal information held in public registers for the purposes of the *Corporations Act* provided a specific example of a more general issue—that is, 'finding the appropriate balance in granting access to, and setting limits upon the subsequent use of, information held on public registers'.[184] The OPC submitted that the availability of personal information held in public registers has been the subject of complaints and enquiries, but recognised the public policy objectives behind making such information publicly available. It argued:

> The balance between maintaining the privacy of this information and meeting the important public policy objectives might be better achieved by more narrowly specifying in the Corporations Act the purposes for which such information may be used, particularly in regard to shareholder registers.[185]

16.131 The OPC offered in-principle support for the idea of using trusted third-party 'clearing houses' to manage contact between individuals on registers and third parties. In the OPC's view, avoiding the need to provide personal information directly to the requesting party would address the risk that the information may be misused or

---

181 Senate Disallowable Instruments List (as at 1 April 2008): A notice of motion to disallow the *Corporations Amendment Regulations 2007 (No 9)* (Cth) was given by a Senator during the last (41st) Parliament. This notice was not resolved at the time that the Parliament was prorogued for the 2007 federal election. As a consequence, under s 42(3) of the *Legislative Instruments Act 2003* (Cth), the *Corporations Amendment Regulations 2007 (No 9)* (Cth) is taken to be tabled in the Senate on the first sitting day of the new (42nd) Parliament, that is 12 February 2008.

182 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(j).

183 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.83]–[13.92]. See also Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(j).

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

185 Ibid.

mishandled. It noted that the *Corporations Amendment Regulation 2007 (No 9)* would provide for such a mechanism.[186]

16.132 The Australian Government Treasury noted, however, that the underlying rationale for providing access to registers of members was to facilitate 'informed dealings by members and prospective members, and other stakeholders'.[187] The Treasury argued, in relation to members, that 'public access to the register promotes effective participation in the key democratic processes in a company' and that restricting public access to the register could lead to 'underperformance and reduced market efficiency'. The Treasury also stressed the need for members of the public interested in acquiring shares in a company (for example, through a takeover offer) to be able to find out the identity of the present owners of a company.[188]

16.133 The Treasury disagreed with the OPC's suggestion that the provisions of the *Corporations Regulations* limiting access to registers of members of mutuals should be extended to all companies.[189]

> The limitations on access to the registers of members of mutuals are adapted to the special circumstances surrounding membership of such institutions. Some mutuals have a customer base concentrated in security sensitive areas such as the defence and police forces. Provisions of the *Banking Act 1959* prevent customers of financial institutions from using a non-residential address when opening an account. Members of companies other than mutual financial institutions have the options [sic] of specifying a non-residential address, such as a post office box, to the extent that they have concerns about their personal security…
>
> The limitations on access to registers of members of mutuals may have an adverse effect on the accountability of the management of those bodies to their members. In the case of mutuals, that disadvantage is outweighed by the need to ensure the personal security of members. In our view extension of similar limitations to all companies would have significant costs that would not be justified by the benefits of such a regulatory intervention. [190]

ALRC's view

16.134 The ALRC does not make a recommendation in relation to the use and disclosure of personal information held on a register of members. The *Corporations Act* provides significant protection for personal information held on a register. These protections strike an appropriate balance between the right of the public to know about, and use, information from a register, and the policy that shareholders should be free from undue intrusion from the use of such information. The ALRC also notes that the member registers of mutuals, such as credit unions, receive extra protection under the *Corporations Regulations.* They will receive further protection if the *Corporations Amendment Regulations 2007 (No 9)* come into effect.

---

186 Ibid. The OPC noted that, at the time of making its submission, the regulation had been the subject of a disallowance motion prior to Parliament being prorogued.

187 Australian Government Treasury, *Submission PR 581*, 20 March 2008.

188 Ibid.

189 Ibid.

190 Ibid.

16.135 The *Privacy Act* also provides some protection for personal information held on a register of members.[191] For example, under the current law, the collection by an organisation of information from a register is subject to NPP 1. Personal information included on a register is subject to the data-quality requirements of NPP 3. Such protection will continue under the model UPPs. The application of the *Privacy Act* to publicly available information is discussed further in Chapter 11.

Commonwealth Electoral Act 1918 (Cth)

16.136 The *Commonwealth Electoral Act 1918* (Cth) and the *Privacy Act* provide the legislative privacy framework governing the Commonwealth electoral roll. Part VI of the *Commonwealth Electoral Act* provides for the establishment of an electoral roll. Under s 101 of the Act, it is compulsory for all eligible persons in Australia to maintain continuous enrolment on the Commonwealth electoral roll for the purposes of federal elections and referendums. The names and addresses of all electors on the Commonwealth electoral roll are available for public inspection in various formats specified under the *Commonwealth Electoral Act*.[192] The Act also requires the Australian Electoral Commission (AEC) to provide electoral roll information to a number of different individuals and organisations, including members of Parliament and registered political parties.[193]

16.137 Section 91A of the *Commonwealth Electoral Act* provides that a person or organisation that obtains information from the electoral roll must not use it except for a permitted purpose. The permitted purposes in relation to a political party include: any purpose in connection with an election or referendum; research regarding electoral matters; and monitoring the accuracy of information contained in a roll. Disclosure to political organisations for these permitted purposes would be authorised by law for the purposes of the *Privacy Act*.[194]

16.138 One issue for consideration is whether the provisions under the *Commonwealth Electoral Act* and the *Privacy Act* provide adequate protection for personal information—particularly information provided to political organisations.[195] Although the *Commonwealth Electoral Act* regulates what electoral roll information can be provided to individuals and organisations, and how they can use the information, it does not provide for other information privacy protection such as data security and retention. These issues are dealt with in the NPPs. The NPPs do not, however, apply to acts or practices carried out by political organisations and their contractors, subcontractors and volunteers in relation to electoral matters.[196]

---

191 *Privacy Act 1988* (Cth) s 16B.
192 *Commonwealth Electoral Act 1918* (Cth) ss 90, 90A.
193 Ibid s 90B.
194 *Privacy Act 1988* (Cth) s 14, IPP 10.1(c).
195 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(k).
196 *Privacy Act 1988* (Cth) s 7C. The application of the *Privacy Act* to registered political parties and political acts and practices is discussed in detail in Ch 41.

16.139 In IP 31, the ALRC asked whether the *Commonwealth Electoral Act* provided adequate protection of personal information included on the electoral roll.[197] The OPC submitted that protection consistent with the principles contained in the *Privacy Act* should be afforded to the handling of information from the electoral roll, particularly in regard to those bodies that may handle such information but which are not regulated under the *Privacy Act*.[198]

16.140 Some stakeholders submitted that amendments to the *Commonwealth Electoral Act* have resulted in personal information on the electoral roll being used for a purpose other than the primary purpose for which it was collected. In particular, the Australian Privacy Foundation submitted that the electoral roll is now a resource for identity verification. This is the case particularly in relation to the new obligations under the AML/CTF Act.[199]

16.141 The OPC also reported concerns in the community about the use of information obtained from old electoral rolls, in particular, the use of the information for direct marketing and by debt collectors. In one case, a debt collector, acting on behalf of a psychiatrist, allegedly sent an account on the psychiatrist's letterhead to the debtor's work address. In another case, a debt collector allegedly sent letters of demand to all persons of the same name listed on the electoral roll in an attempt to recover a debt.[200]

16.142 There was, however, some support for greater access to the electoral roll. The Institute of Mercantile Agents, for example, noted that the cost of debt arising from unlocated account holders is passed on to consumers. It submitted that the prohibition on the use of electoral roll information to locate debtors costs consumers over $4 billion.[201]

16.143 The OPC noted that a range of agencies can obtain access to the electoral roll. Under the *Electoral and Referendum Regulations 1940* (Cth), 22 Australian Government agencies are authorised to use information on the electoral roll for a range of regulatory, law enforcement and public revenue purposes.[202] In the OPC's view, given the mandatory nature of enrolment, it is appropriate that access to the electoral roll remain relatively narrow.[203]

16.144 Stakeholders also expressed concern about the use of information from other agencies to update the roll. Under s 92 of the *Commonwealth Electoral Act*, the AEC has substantial powers to collect personal information from a range of Australian Government and state and territory agencies to maintain the integrity of the electoral roll. Updating the roll would include, for example, matching personal information from

197 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(k).
198 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
199 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.
200 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
201 Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.
202 *Commonwealth Electoral Act 1918* (Cth) sch 1.
203 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

another source with the personal information held on the electoral roll. The OPC submitted that:

> In the context of the Electoral Roll, it may be appropriate that any data-matching only be pursued where appropriate regard for privacy issues has been given. In particular, the purpose of the data-matching should be narrowly defined as being to maintain the accuracy of the Electoral Roll. Further, formal protocols may be required to ensure that redundant or unmatched personal information is not retained.[204]

The political exemption and electoral roll information

16.145 In DP 72, the ALRC stated that the compulsory provision of information for the electoral roll requires that an appropriate balance be struck between the public interest in ensuring transparent electoral procedures and the public interest in protecting privacy.[205] The ALRC expressed the preliminary view that the *Commonwealth Electoral Act* and the *Privacy Act* balance these interests appropriately.[206]

16.146 The ALRC noted that it was concerned, however, that, due to the interaction between the *Commonwealth Electoral Act* and the exemptions under the *Privacy Act*, political organisations and their contractors, subcontractors and volunteers, are not subject to any rules relating to secure storage and retention of personal information held on the electoral roll.[207]

16.147 The ALRC proposed that, in the event that the exemption under the *Privacy Act* that applies to registered political parties and political acts and practices is not removed, the *Commonwealth Electoral Act* should be amended to provide that prescribed individuals, authorities and organisations, to whom the AEC must give information in relation to the electoral roll and certified lists of voters, must: take reasonable steps to protect the information from misuse and loss, and from unauthorised access, modification or disclosure; and destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.[208]

16.148 While there was some support from stakeholders for the proposed amendment to the *Commonwealth Electoral Act*,[209] a number argued that it was preferable that the exemption for political parties be removed from the *Privacy Act*.[210]

ALRC's view

16.149 The issues raised in relation to the use of electoral roll information are best addressed by the removal of the political exemption from the *Privacy Act.* In

---

204 Ibid.
205 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.93].
206 Ibid.
207 Ibid, [13.94].
208 Ibid, Proposal 13–1.
209 Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Queensland Government, *Submission PR 490,* 19 December 2007.
210 Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

Chapter 41, the ALRC recommends that the *Privacy Act* be amended to remove the exemption for registered political parties and the exemption for political acts and practices.[211]

16.150 In the event that the exemption under the *Privacy Act* that applies to registered political parties and political acts and practices is not removed, however, the *Commonwealth Electoral Act* should be amended to provide that prescribed individuals, authorities and organisations, to whom the AEC must give information in relation to the electoral roll and certified lists of voters, must take reasonable steps to:

- protect the information from misuse and loss and from unauthorised access, modification or disclosure; and
- destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.

Uses other than for the primary purpose of collection

16.151 In DP 72, the ALRC acknowledged concerns raised by the OPC about the use of data-matching to update the electoral roll, and the retention of redundant or unmatched personal information.[212] The ALRC proposed that the AEC and state and territory electoral commissions, in consultation with the OPC, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.[213]

Submissions and consultations

16.152 This proposal was supported by almost all of the stakeholders that addressed the issue.[214] The OPC again expressed concern about the broad and general powers of demand under the *Commonwealth Electoral Act*, which it argued may be excessive and unnecessary for purposes of updating the electoral roll.[215] The OPC recommended that state and territory privacy and information commissioners also be involved in the development of protocols regarding the handling of personal information pursuant to continuous roll update.[216] This view was shared by the OVPC, which submitted that:

> while some limited scope for collection, use and disclosure of personal information for political and electoral purposes is desirable in a parliamentary democracy, this should be achieved in such a way as to maximise the protection afforded to the personal information involved and minimise the risks to privacy.[217]

---

211 Rec 41–1.
212 See, eg, Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
213 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 13–2.
214 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; Queensland Government, *Submission PR 490*, 19 December 2007; Australia Post, *Submission PR 445*, 10 December 2007.
215 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
216 Ibid.
217 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

16.153 The ABA and the Investment and Financial Services Association (IFSA) submitted that the Privacy Commissioner should consult stakeholders when developing protocols.[218] IFSA argued that this was necessary to facilitate a comprehensive understanding of the purposes for which information on the electoral roll is used—for example, superannuation providers often use electoral roll information as a tool to locate 'lost members'.[219]

ALRC's view

16.154 There is merit in the development of protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll. The AEC and state and territory electoral commissions should develop and publish protocols. This should occur in consultation with the OPC as well as state and territory privacy commissioners and agencies with responsibility for privacy regulation. The wider consultation process is a matter for the AEC and state and territory electoral commissions, however, they should note the views expressed by stakeholders to this Inquiry concerning such a process.

Recommendation 16–3 The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, state and territory privacy commissioners and agencies with responsibility for privacy regulation, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

Overview of the requirements of the AML/CTF Act

Background

16.155 The AML/CTF Act received Royal Assent on 12 December 2006. The Act requires a 'reporting entity' to carry out a procedure to verify a customer's identity before providing a 'designated service' to the customer.[220] In addition, reporting entities must give the Australian Transaction Reports and Analysis Centre

218 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

219 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007. Australia Post submitted that it should be noted as a stakeholder in the process: Australia Post, *Submission PR 445*, 10 December 2007.

220 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) pt 2. The terms 'reporting entity' and 'designated service' are considered below.

(AUSTRAC) reports about suspicious matters;[221] and must develop and comply with an anti-money laundering and counter-terrorism financing program.[222]

16.156 The AML/CTF Act is the result of an extensive consultation process. On 16 December 2005, the AGD released the exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill (the exposure Bill) along with draft Rules.[223] The AGD received 120 submissions on the exposure Bill. The exposure Bill was referred to the Senate Legal and Constitutional Legislation Committee. The Committee reported on its inquiry on 13 April 2006.[224] The Committee concluded that an independent PIA of the Bill should be conducted. The Committee also recommended that the Bill should contain a statement that is reflective of the intention to allow federal, state and territory agencies to access and utilise AUSTRAC data for purposes that may not be related to anti-money laundering or counter-terrorism financing, such as detecting tax and social security fraud.[225]

16.157 The AGD released a revised exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) (revised AML/CTF Bill 2006) and draft Rules for a further period of consultation, which ended on 4 August 2006.[226] The Department received a further 70 submissions on the revised AML/CTF Bill 2006. Submissions in response to the revised AML/CTF Bill 2006 raised a number of privacy issues.

16.158 In September 2006, an independent PIA was conducted, in which 96 recommendations were made.[227] The Australian Government then published a Privacy Impact Statement which responded to the PIA findings and recommendations. The Government adopted 30 of the 96 recommendations.[228]

16.159 The final version of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) (AML/CTF Bill 2006) was introduced in the Australian Parliament on 1 November 2006. The final version of the Bill required that designated agencies, including state and territory agencies, comply with the IPPs in respect of the accessed AUSTRAC information.

---

221 Ibid pt 3.

222 Part A of an anti-money laundering and counter-terrorism financing program is a program that is designed to identify, mitigate and manage the risk a reporting entity reasonably may face when providing designated services in Australia that might involve or facilitate money laundering or financing of terrorism. Part B of an anti-money laundering and counter-terrorism financing program sets out the applicable customer identification procedures for customers of the reporting entity: Ibid s 80.

223 See Australian Government Attorney-General's Department, *Anti-money laundering* <http://www.ag.gov.au/www/agd/agd.nsf/Page/Anti-money_laundering> at 6 May 2008.

224 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005* (2006).

225 Ibid, [4.72]–[4.76].

226 Revised Exposure Draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth).

227 Salinger & Co, *Privacy Impacts of the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules* (2006). See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.105] for a summary of the key recommendations.

228 Australian Government Attorney-General's Department, *Privacy Impact Statement: Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules* (2006).

16.160 After its introduction, the AML/CTF Bill was referred to the Senate Legal and Constitutional Legislation Committee. Submissions to the Senate Committee continued to raise privacy issues. The Committee reported on its inquiry on 28 November 2006. The Committee recommended that the Australian Government consider amending the Bill to include further threshold value limits, to exclude low risk, low value services (such as the provision of travellers cheques and foreign currency transactions) from the definition of 'designated services' and that consideration be given to indexing these thresholds every five years. The Committee also recommended that the OPC conduct periodic audits of AUSTRAC's compliance with privacy obligations in its administration of the Bill.[229]

Current requirements under the AML/CTF Act

16.161 The AML/CTF Act is intended to enable individual businesses to manage money laundering and terrorism financing risks. The Act sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person that provides 'designated services'.[230] A large number of 'designated services' are listed in the Act including opening an account, making a loan, and supplying goods by way of hire purchase.[231]

16.162 As stated above, the Act requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer.[232] Reporting entities must give AUSTRAC reports about suspicious matters;[233] and must develop and comply with an anti-money laundering and counter-terrorism financing program.[234] The Act also imposes various record-keeping requirements on reporting entities.[235] For example, a reporting entity must make a record each time it provides a designated service and must retain the record for seven years.[236]

16.163 Part 11 of the Act relates to secrecy and access. Except as permitted by the Act, certain individuals—including an AUSTRAC official, a customs officer or a police officer—must not disclose information or documents obtained under the Act.[237] Further, a reporting entity must not disclose that it has reported, or is required to report, information to AUSTRAC; or that it has formed a suspicion about a transaction or matter. The Part also provides that the ATO and certain other 'designated agencies'

---

229 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]* (2006). None of these recommendations have been implemented to date.

230 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5.

231 Ibid s 6.

232 Ibid pt 2.

233 Ibid pt 3.

234 Part A of an anti-money laundering and counter-terrorism financing program is a program that is designed to identify, mitigate and manage the risk a reporting entity may reasonably face when providing designated services in Australia that might involve or facilitate money laundering or financing of terrorism. Part B of an anti-money laundering and counter-terrorism financing program sets out the applicable customer identification procedures for customers of the reporting entity: Ibid s 80.

235 Ibid pt 10.

236 Ibid s 107.

237 Ibid pt 11, div 2.

may obtain access to AUSTRAC information. The phrase 'designated agencies' is defined in s 5 to include a large number of Australian Government agencies as well as some state and territory agencies. Designated agencies may obtain access to AUSTRAC information for the purposes of performing that agency's functions and exercising the agency's powers.[238] The Act requires designated agencies, including state and territory agencies, to comply with the IPPs in respect of AUSTRAC information.[239]

16.164 The *Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006* (Cth) was assented to on the same day as the AML/CTF Act. The *Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act* introduced s 63(1A) into the *Privacy Act.* This provision has the effect of making a small business operator that is a reporting entity (a person who provides a designated service under the AML/CTF Act) an organisation for the purposes of the *Privacy Act*. This ensures that all reporting entities are subject to the *Privacy Act* in relation to their obligations to collect personal information under the AML/CTF Act.

16.165 The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2007* (Cth) made a number of amendments to the AML/CTF Act and other legislation. In particular, it amended the *Commonwealth Electoral Act 1918* to provide that a prescribed person or organisation, that under an arrangement with a reporting entity or the agent of a reporting entity, provides information for the purpose of facilitating the carrying out of the applicable customer identification procedures under the AML/CTF Act, will have access to the electoral roll 'equivalent to that which is currently provided for the purposes of the *Financial Transactions Reports Act 1988*'.[240]

16.166 The AML/CTF Act represents the first tranche of reforms under the anti-money laundering and counter-terrorism legislative scheme, which covers the financial and gambling sectors.[241] The second tranche of reforms is currently being developed.[242] The second tranche will extend the existing regulatory obligations to specified transactions 'conducted by real estate agents, specified transactions conducted by dealers in precious metals and precious stones and specified legal, accounting and trust and company services'.[243] Draft legislative provisions which will amend the AML/CTF Act to implement the second tranche of reforms were publicly released in August 2007.[244] Public submissions have now closed and the AGD is

238 Ibid s 126.
239 Ibid s 126(3).
240 Explanatory Memorandum, Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2007 (Cth), item 54; Commonwealth, *Parliamentary Debates*, House of Representatives, 15 February 2007, 1 (P Ruddock—Attorney-General) *Anti-Money Laundering and Counter-Terrorism Financial Amendment Bill 2007* Second Reading Speech, 1.
241 Australian Government Attorney-General's Department, *Second Tranche of Reforms—Second Tranche of AML/CTF Reforms* (2007) <www.ag.gov.au/www/agd/agd.nsf/Page/Anti-moneylaundering_SecondTrancheofReforms> at 1 April 2008.
242 Ibid.
243 Ibid.
244 Ibid.

consulting with peak bodies representing the relevant professions about the draft legislative provisions.[245]

Concerns about the AML/CTF legislation

16.167 In DP 72, the ALRC noted that stakeholders had raised a number of issues in relation to the AML/CTF Act. Concerns were raised that privacy was not adequately protected under the AML-CTF legislation and that its measures would lead to pervasive monitoring of the financial affairs of ordinary citizens. Another concern was that state and territory agencies may obtain access to information collected by AUSTRAC without being subject to the same accountability under the *Privacy Act* as Australian Government agencies. Also raised was that designated agencies had been granted access to AUSTRAC data, using information for purposes outside of the intentions of anti-money laundering and counter-terrorism financing legislation. A further issue was the need for the $10,000 mandatory reporting thresholds to be reviewed to reflect price inflation and minimise the unnecessary collection of personal information.[246]

16.168 A number of submissions from financial institutions and peak industry bodies noted that the AML/CTF Act requires a reporting entity to carry out a procedure to verify a customer's identity prior to providing a designated service, but does not expand access to available databases for identity verification purposes.[247] Some submissions raised the issue of using credit reporting information for the purposes of identity verification.[248]

Statutory review

16.169 In DP 72, the ALRC noted that there have been several recent inquiries that have considered the AML/CTF Act, in which issues of concern have been comprehensively put to government. The ALRC, therefore, restricted its consideration of the Act to issues raised in submissions to this Inquiry. The ALRC indicated that it shares many of the concerns raised by stakeholders in relation to the AML/CTF Act.

16.170 The ALRC noted that, under s 251 of the AML/CTF Act, the Minister responsible for the Act must cause a review to be conducted of the operation of the Act, the regulations and the AML/CTF Rules, before the laws have been in operation for seven years.

16.171 In DP 72, the ALRC proposed that the review under s 251 should examine whether:

- reporting entities and designated agencies are handling personal information appropriately under the legislation;

---

245 Ibid.

246 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [13.110]–[13.116].

247 Ibid, [13.117].

248 This issue is discussed briefly below and in detail in Ch 57.

- the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;
- it remains appropriate that reporting entities are required to retain information for seven years; and
- it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification.[249]

16.172 The use of the electoral roll for the purpose of complying with the AML/CTF Act is discussed above.

Submissions and consultations

16.173 The majority of stakeholders who commented on this issue supported the ALRC's proposal.[250] The OPC submitted that the review also should include the handling of information by AUSTRAC, particularly as it relates to the provision of access to other bodies, including those overseas. The OPC commented that it was prudent for relevant stakeholders, including AUSTRAC and the OPC, to begin retaining appropriate data to assist in the review.[251]

16.174 A number of stakeholders, however, called for the ALRC to make recommendations in relation to possible amendments to the AML/CTF Act to protect privacy better. For example, the Law Council of Australia indicated that, while it understood the reluctance of the ALRC to 'reignite debate on an Act that was only passed relatively recently and which was the subject of extensive consultation and discussion',[252]

> the current AML/CTF Act represents stage one of a two stage reform process. It will soon be amended to cover the provision of a broader range of services, including legal and accounting services. It is of limited assistance to those currently engaged in consultation on the form and content of stage two reforms to note that the ALRC acknowledges privacy concerns with the existing Act but believes that they should only be the subject of review in six years time …
>
> The Law Council would welcome more immediate guidance from the ALRC on how the AML/CTF Act could be brought into line with the *Privacy Act*. [253]

16.175 The ABA noted that banks already have to comply with these laws, and that the statutory review under s 251 of the AML/CTF Act would not occur until 2014.[254]

---

249 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 13–3.

250 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; 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.

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

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

253 Ibid.

254 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

The ABA and the National Australia Bank called for the ALRC to reconcile the existing AML/CTF legislation with proposed privacy reforms.[255]

16.176 The ABA cited two examples of possible inconsistency between the AML/CTF laws and existing privacy law and practice. First, the ABA contended that OPC guidance on the AML/CTF Act was at odds with s 123 of the Act, which requires a reporting entity not to make a disclosure to a person in relation to suspicious matters. The ABA stated that it has been advised by the AGD that the AML/CTF Act overrides the *Privacy Act*.[256] The ABA submitted that banks are concerned about branch staff being caught between the two in absence of case law on point.[257]

16.177 Secondly, in relation to employee due diligence, the ABA noted that the AML/CTF Rules include a note referring reporting entities to the Privacy Commissioner's information sheet in relation to the handling of employee information, but no specific information sheet exists. The ABA pointed out that a risk-based Employee Due Diligence program could be inconsistent with NPP collection obligations.[258]

ALRC's view

16.178 It is clear that there is a high level of concern about the erosion of privacy generated by the AML/CTF Act. While the ALRC has been requested by stakeholders to address the issues raised by the Act, in the ALRC's view, it should not accede to this request for two reasons. First, a number of recent inquiries have considered the issues raised by the AML/CTF Act. Secondly, while the ALRC shares many of the concerns raised by stakeholders in relation to the AML/CTF Act, to review comprehensively the AML/CTF Act is beyond the scope of this Inquiry. For these reasons, the ALRC has restricted its consideration of the Act to some of the issues raised in submissions to this Inquiry.

16.179 The ALRC suggests that the OPC review its guidance on the AML/CTF Act so as to address the concerns expressed by the ABA about inconsistencies between this guidance and the requirements of the Act itself. The ALRC notes, for example, that the guidance published by the OPC states:

> *What are my reporting obligations in relation to providing individuals with access?*
>
> Access should be provided, unless there is a legitimate exception. For example, a reporting entity may be able to deny access to a suspicious matter report lodged with AUSTRAC under NPP 6.1(h).
>
> Reporting entities are required to tell individuals why they are denying access to some or all of their personal information.[259]

---

255 Ibid; National Australia Bank, *Submission PR 408*, 7 December 2007.
256 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.
257 Ibid.
258 Ibid.
259 Office of the Privacy Commissioner, *Privacy and the AML/CTF Act—some FAQs for your business*, October 2007, 2.

16.180 There is a reasonable argument that, if a reporting entity advised an individual that it could not disclose personal information which formed part of a suspicious matter report, it would be in breach of s 123 of the AML/CTF Act. In relation to the second point raised by the ABA, however, the ALRC notes that Information Sheet 16 issued by the OPC, deals with disclosure of personal information about employees in the context of due diligence.[260]

16.181 The ALRC is concerned about the pervasive nature of the monitoring that is to occur due to the mandatory reporting threshold of $10,000. As suggested by the OPC, the threshold should be reviewed to reflect price inflation and minimise the unnecessary collection of personal information.

16.182 The statutory review under s 251 of the AML/CTF should examine: whether reporting entities and designated agencies are appropriately handling personal information under the legislation; whether the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation; and whether it remains appropriate that reporting entities are required to retain information for seven years.

16.183 The review also should consider whether the use of the electoral roll by reporting entities for the purpose of identity verification is appropriate.[261] Consideration should also be given to allowing the AEC to provide reporting entities with other information—for example, date of birth information—so as to reduce the need for credit reporting information to be used for the purposes of identity verification under the AML/CTF Act.[262]

16.184 The ALRC agrees with the OPC that the review under s 251 of the AML/CTF Act also should consider the handling of information by AUSTRAC, particularly as it relates to the provision of access to other bodies, including those overseas.

Recommendation 16–4 The review under s 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) should consider, in particular, whether:

(a) reporting entities and designated agencies are handling personal information appropriately under the legislation;

---

260 Office of the Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (October 2002), 3.

261 The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2007* (Cth) amended the *Commonwealth Electoral Act 1918* to provide that a prescribed person or organisation, that under an arrangement with a reporting entity or the agent of a reporting entity, provides information for the purpose of facilitating the carrying out of the applicable customer identification procedures under the AML/CTF Act, will have access to the electoral roll.

262 The use of credit reporting information for the purposes of electronic identity verification is discussed in Ch 57. There is an argument that it may be preferable, for example, to allow the use of personal information from the electoral roll for the purposes of electronic identity verification, rather than allowing the use of credit reporting information for this purpose.

(b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;

(c) it remains appropriate that reporting entities are required to retain information for seven years;

(d) the use of the electoral roll by reporting entities for the purpose of identification verification is appropriate; and

(e) the handling of information by the Australian Transaction Reports and Analysis Centre is appropriate, particularly as it relates to the provision of access to other bodies, including bodies outside Australia.

State and territory agencies

16.185 In DP 72, the ALRC stated that it also was concerned about the number of designated agencies granted access to AUSTRAC data collected under the AML/CTF Act, and the limited protection offered by s 126(3) of the Act. The ALRC expressed the preliminary view that, due to the amount of personal information that will be made available to the agencies, it is appropriate that these agencies should have to comply with the relevant privacy principles in relation to that information.

16.186 The ALRC noted that, while the agencies must agree to be bound by the IPPs, the Privacy Commissioner does not have the power to audit or enforce compliance with the IPPs by state and territory agencies. The ALRC proposed, therefore, that the AML/CTF Act should be amended to provide that state and territory agencies that have access to personal information provided to AUSTRAC, be regulated under the *Privacy Act* in relation to the handling of that personal information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act*.[263]

Submissions and consultations

16.187 The OPC supported this proposal, as did a number of other stakeholders.[264] The OPC noted that, currently, only some states and territories have privacy regulation applying to their own agencies.

> As this personal information is compulsorily acquired during the course of an expanding range of transactions, in some instances without the knowledge of the individual, it seems reasonable to expect that agencies which receive it are subject to binding privacy obligations. Currently, state and territory agencies in a number of jurisdictions represent a gap in the privacy protections afforded to AML/CTF information, in particular since the enactment of provisions to bring small business

263 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 13–4.

264 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; 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; P Youngman, *Submission PR 394*, 7 December 2007.

> reporting entities within the coverage of the *Privacy Act*. Essentially, all participating private sector organizations and Australian Government agencies are covered by enforceable privacy regulation, though not all State and Territory agencies.

16.188 The OPC also proposed that it have responsibility for assessing whether state and territory legislation contains obligations that are at least the equivalent of all the relevant obligations in the *Privacy Act*.[265] The Queensland Government submitted that this issue should be considered within the context of developing and implementing a nationally consistent approach.[266]

ALRC's view

16.189 The ALRC is concerned about the number of designated agencies that have been granted access to AUSTRAC data collected under the AML/CTF Act and the limited protection offered by s 126(3) of the Act. Due to the amount of personal information that will be made available to such agencies, it is appropriate that these agencies comply with the model UPPs.

16.190 This is most appropriately addressed by the ALRC's recommendation that the states and territories should enact legislation regulating the handling of personal information in that state or territory's public sector that applies the model UPPs.[267] Further, 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.[268]

16.191 Until such a cooperative scheme is in place, when AUSTRAC provides a state or territory agency with access to AUSTRAC data collected under the AML/CTF Act, it should ensure that a memorandum of understanding or other arrangement is in place to ensure compliance with the privacy requirements of the AML/CTF Act. The OPC should monitor compliance with the privacy requirements of the AML/CTF Act by such state and territory agencies. This is consistent with the general approach recommended by the ALRC.[269]

---

265 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
266 Queensland Government, *Submission PR 490*, 19 December 2007.
267 Rec 3–4.
268 Rec 3–6.
269 Rec 17–1.

17. Interaction with State and Territory Laws

Contents

Introduction

17.1 In this chapter the ALRC considers how the *Privacy Act 1988* (Cth) interacts with state and territory privacy laws. A number of examples of inconsistency between the *Privacy Act* and privacy regimes that regulate state and territory public sectors are first identified. The regulation of personal information handled by intergovernmental bodies is considered and the role of state and territory privacy regulators under nationally consistent privacy laws is outlined. Inconsistency and fragmentation in privacy rules, codes and guidelines are then examined. The final section of the chapter considers the regulation of residential tenancy databases (RTDs).

Interaction of federal, state and territory regimes

17.2 In the absence of a clear statement in the *Australian Constitution* about whether the regulation of personal information is the responsibility of the Australian Government or state and territory governments, the states and territories are able to enact privacy laws.[1] Further, s 3 of the *Privacy Act* states that the Australian Parliament does not intend to 'cover the field' in relation to the protection of personal information.[2] Chapter 2 provides an overview of state and territory privacy laws.

17.3 State and territory laws are sometimes inconsistent with the *Privacy Act* and with each other. This section of the chapter considers the interaction of state and

1 The Constitutional basis for enacting the *Privacy Act 1988* (Cth) was the Australian Government's power to make laws in relation to 'external affairs': *Privacy Act 1988* (Cth) Preamble; *Australian Constitution* s 51(xxix).

2 *Privacy Act 1988* (Cth) s 3 and the *Australian Constitution* are discussed in Ch 4.

territory privacy laws with the *Privacy Act*. It outlines a number of examples of inconsistency between federal, state and territory laws including inconsistencies in relation to terms and definitions; state-owned corporations; contracted service providers; ministers, local governments and universities; the type of personal information regulated; privacy principles; and remedies. These issues are dealt with in detail in other chapters of this Report.

Inconsistent principles

17.4 Although the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) and privacy principles under state and territory privacy regimes are similar, they are not identical. The privacy regimes in some jurisdictions include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs.[3] As is noted in Chapter 18, there are significant differences between the IPPs and the NPPs.

17.5 Many of the differences between the IPPs and the NPPs are reproduced in the state and territory regimes. For example, like the NPPs, the Information Privacy Principles under the *Information Privacy Act 2000* (Vic) include principles relating to anonymity and cross-border data flows.[4] The Information Standard that applies to the Queensland public sector does not provide for either of these principles,[5] but the Information Standard that applies to the Queensland Department of Health does.[6]

17.6 The adoption of the model Unified Privacy Principles (UPPs) and any relevant regulations that modify the application of the UPPs at the federal, state and territory level will deal with many of the problems caused by inconsistent privacy principles across the jurisdictions.[7]

Terms and definitions

17.7 Terms and definitions vary across federal, state and territory laws. For example, each of the state and territory regimes contains definitions of 'personal information' that are similar to the definition of the term under the *Privacy Act*, but not identical.[8]

---

3 See discussion in Ch 2.

4 *Information Privacy Act 2000* (Vic) sch 1.

5 Queensland Government, *Information Standard 42—Information Privacy* (2001).

6 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001), [3.1.8], [3.1.9].

7 See Rec 3–4.

8 See, eg, *Privacy Act 1988* (Cth) s 16B; *Privacy and Personal Information Protection Act 1998* (NSW) s 4; *Information Privacy Act 2000* (Vic) s 3; *Personal Information Protection Act 2004* (Tas) s 3; see definition of 'record' in Queensland Government, *Information Standard 42—Information Privacy* (2001); *Personal Information Protection Act 2004* (Tas) s 4. The *Freedom of Information Act 1992* (WA) refers to personal information contained in documents: see, eg, *Freedom of Information Act 1992* (WA) s 29. The South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992) refers to personal information concerning the 'record subject'. It is, however, unclear whether the instruction covers only documents in a recorded form.

17.8 The inconsistent use of terms and definitions in privacy legislation contributes to the complexity of privacy law and may increase compliance burden and cost. The federal, state and territory governments should ensure the consistency of definitions and key terms (for example, 'personal information', 'sensitive information' and 'health information') in federal, state and territory legislation that regulates the handling of personal information.

17.9 In Chapter 3, the ALRC recommends that the states and territories should enact legislation regulating the handling of personal information in that state or territory's public sector that applies relevant definitions used in the *Privacy Act*. These definitions would include definitions of 'personal information', 'sensitive information' and 'health information'.[9]

Personal information regulated

17.10 Employee records are currently excluded from the operation of the *Privacy Act*.[10] Some state and territory privacy regimes provide limited protection for employee records.[11] The Personal Information Protection Principles under the *Personal Information Protection Act 2004* (Tas) provide the highest degree of protection of employee records, subject to a number of exceptions.[12] In Chapter 40, the ALRC recommends that the current exemption under the *Privacy Act* relating to employee records should be removed. In the ALRC's view, state and territory legislation should include provisions that address the handling of employee records in that state or territory's public sector.

17.11 The *Privacy Act* provides limited protection for information held in public registers. IPP 1 places some restrictions on the collection of personal information in a generally available publication.[13] Similarly, the *Information Act 2002* (NT) provides limited protection for information held in public registers.[14] Other jurisdictions, however, provide greater protection. For example, public registers in Victoria are subject to the Information Privacy Principles under the *Information Privacy Act 2000* (Vic),[15] and the New South Wales legislation prohibits certain disclosures of personal information held in a public register.[16] The issue of publicly available information is discussed in Chapter 6 and Chapter 11.

---

9 See Ch 3 and Rec 3–4.

10 *Privacy Act 1988* (Cth) s 7B(3).

11 See, eg, *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(j); M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005).

12 *Personal Information Protection Act 2004* (Tas) s 10.

13 Similar protection is offered under the Queensland Government, *Information Standard 42—Information Privacy* (2001), [3.1.1].

14 *Information Act 2002* (NT) s 68.

15 *Information Privacy Act 2000* (Vic) s 16(4).

16 *Privacy and Personal Information Protection Act 1998* (NSW) pt 6.

Remedies

17.12 The remedies available to individuals whose privacy rights are infringed can differ according to the jurisdiction in which the complaint is made. For example, the maximum amount of compensation that is payable for an interference with privacy differs across the states and territories. The *Privacy Act* does not specify a limit on the payment of compensation. In contrast, the New South Wales Administrative Decisions Tribunal can order the payment of compensation of up to $40,000;[17] the Victorian Civil and Administrative Tribunal can order compensation of up to $100,000;[18] and the Northern Territory Information Commissioner can order compensation up to $60,000.[19] There is no specific provision for compensation under the *Personal Information Protection Act 2004* (Tas),[20] or under the Queensland privacy scheme.

17.13 In Chapter 50, the ALRC examines various issues related to the enforcement of the *Privacy Act*, including the payment of compensation and whether certain interferences with privacy should attract a civil penalty. To ensure a level of consistency in the outcome of privacy regulation, the states and territories should consider the range of enforcement tools, and the level of penalties and compensation, available under the *Privacy Act* and other state and territory privacy laws when developing privacy legislation.

State-owned corporations

17.14 While a number of state and territory privacy regimes regulate the handling of personal information by state-owned corporations,[21] they are not regulated in New South Wales. This is significant, as state-owned corporations do not fall within the scope of the private sector provisions of the *Privacy Act* unless they are prescribed by regulation.[22] The exemptions under the *Privacy Act* relating to state and territory authorities and prescribed instrumentalities are discussed further in Chapter 38.

State contracted service providers

17.15 There is also confusion about whether contracted service providers to New South Wales government agencies are caught by the *Privacy Act* or the *Privacy and Personal Information Protection Act 1998* (NSW), or fall into an unregulated gap between the state and federal Acts.[23] In Chapter 14, the ALRC discusses various issues related to state contracted service providers. In Chapter 3, the ALRC recommends that

---

17 Ibid s 55(2)(a).

18 *Information Privacy Act 2000* (Vic) s 43.

19 *Information Act 2002* (NT) s 115.

20 The Tasmanian Ombudsman, however, can make any order that he or she considers appropriate on finding a contravention of a Personal Information Protection Principle: *Personal Information Protection Act 2004* (Tas) s 22.

21 See, eg, *Information Privacy Act 2000* (Vic) s 3; Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].

22 *Privacy Act 1988* (Cth) s 6C(1).

23 See Ibid s 7B(5); *Privacy and Personal Information Protection Act 1998* (NSW) s 4(4)(b); Privacy NSW, *Submission to the New South Wales Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998*, 24 June 2004, 77.

state and territory legislation regulating the handling of personal information in that state or territory's public sector should include provisions relating to state and territory government contracts.

Ministers, local governments and universities

17.16 While legislation in some jurisdictions applies to ministers,[24] the *Privacy and Personal Information Protection Act 1998* (NSW) does not cover ministers and specifically authorises the disclosure of information to ministers and the Premier.[25] The handling of personal information by local governments is regulated under privacy regimes in some states and territories.[26] Local governments are not regulated, however, in Queensland[27] or South Australia.[28]

17.17 Universities are subject to personal information laws in some jurisdictions,[29] but not others.[30] Private universities and universities established under ACT legislation are covered by the *Privacy Act*, as are other private sector higher education providers. This creates further inconsistency in privacy regulation between bodies that substantially provide the same function.[31]

17.18 In Chapter 3, the ALRC recommends that the states and territories enact legislation that applies the UPPs and any relevant regulations that modify the operation of the UPPs.[32] The ALRC envisages that this legislation would include a definition of 'agency' that applies to state and territory ministers, universities, and local governments. This will ensure that these individuals and agencies are subject to the same privacy principles.

Intergovernmental bodies

17.19 The Office of the Privacy Commissioner (OPC) submitted to the Inquiry that:

> The existing definition for 'agency' in the *Privacy Act* may benefit from additional clauses to clarify currently ambiguous areas of coverage. In particular, coverage of some public authorities created as collaborations between the Commonwealth and the States and Territories by the Council of Australian Governments (COAG) and other Ministerial Councils could be better provided for under the definition of agency in the *Privacy Act*.[33]

---

24 See, eg, *Personal Information Protection Act 2004* (Tas) s 3.
25 *Privacy and Personal Information Protection Act 1998* (NSW) s 28(3).
26 For example, Ibid s 3; *Information Privacy Act 2000* (Vic) s 9(1)(d).
27 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1] and *Financial Management Standard 1997* (Qld) s 5(2)(c).
28 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992), 2(2) and *Public Sector Management Act 1995* (SA) s 3.
29 See, eg, *Personal Information Protection Act 2004* (Tas) s 3.
30 See, eg, South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992), 2(2) and *Public Sector Management Act 1995* (SA) s 3.
31 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
32 See Rec 3–4.
33 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

17.20 In DP 72, the ALRC noted that bodies established by cooperative arrangements, such as intergovernmental working groups and officer working groups that assist ministerial councils, often may have to share personal information. The application of privacy regulation to such entities often will be uncertain, as they may not fall within the *Privacy Act* definition of organisation or agency. Equally, they may not be considered state and territory agencies for the purpose of privacy regulation in other jurisdictions.

17.21 To ensure the protection of personal information held by Australian Government agencies, the ALRC proposed that the *Privacy Act* be amended to provide that when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies, the Australian Government agency should ensure that a memorandum of understanding (MOU) is in place. An MOU should help to ensure that the intergovernmental body and its members do not act, or engage in a practice, that would breach the Act.

Submissions and consultations

17.22 A number of stakeholders supported the proposal.[34] The Australian Taxation Office (ATO) noted that the ATO already uses MOUs when it shares personal information with state and territory government bodies. These MOUs impose obligations on the parties to protect personal information in accordance with either the *Privacy Act* or privacy principles specific to their jurisdiction.[35]

17.23 Privacy NSW noted that any such agreement should include a mechanism for complaint handling, dissemination of information about the existence of the agreement, and the means by which individuals can bring complaints against the intergovernmental body.[36]

17.24 The OPC suggested that the definition of 'agency' in the *Privacy Act*, which currently includes a Minister, should describe the specific acts and practices of the Minister that are covered. This would clarify which practices of a Minister are covered and which are exempt.[37]

17.25 The Queensland Government submitted that the requirement should apply only where the participation involves the provision of personal information to the state or territory agency, and that state or territory does not have an equivalent or superior privacy regime (whether statutory or administrative).[38]

---

34 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; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.

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

36 Privacy NSW, *Submission PR 468*, 14 December 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

38 Queensland Government, *Submission PR 490*, 19 December 2007.

17.26 Other stakeholders did not support the proposal. One stakeholder questioned whether the proposal would apply to meetings of Commonwealth and state officials generally, and how the proposal would operate if an intergovernmental body included foreign government representatives.[39] Some stakeholders noted the resource implications of drafting an MOU every time an intergovernmental body was involved in activities which required the handling of personal information. [40]

17.27 The Australian Federal Police submitted that the proposal was unduly prescriptive and unnecessary.

> In a law enforcement context, it is standard operating procedure to only provide personal information to other agencies if it is necessary and if the AFP is satisfied that the other party will take appropriate care of the information. A requirement to codify existing practices in this way may unnecessarily impede operational activity as the proposal appears to go further than the analysis in the discussion paper which focused on policy type working groups.[41]

17.28 The National Transport Council (NTC) submitted that the proposal is unnecessary, as participants in intergovernmental bodies are subject to the *Privacy Act* or state and territory legislation. The NTC suggested that these obligations would not cease to apply when operating in the context of a COAG created body or some other intergovernmental arrangement. The NTC also questioned whether the definition of 'agency' under the *Privacy Act* should cover intergovernmental bodies and COAG created bodies.[42]

ALRC's view

17.29 The application of privacy regulation to bodies established by cooperative arrangements (such as intergovernmental working groups and officer working groups that assist ministerial councils) often will be uncertain, as they may not fall within the *Privacy Act* definition of organisation or agency. Equally, they may not be considered state and territory agencies for the purpose of privacy regulation in other jurisdictions.

17.30 The privacy obligations of participants in intergovernmental bodies should be clear. The ALRC recommends, therefore, that when an Australian Government agency is participating in an intergovernmental body, or other arrangement involving state and territory agencies, that handle personal information, the Australian Government agency should ensure that an MOU or other arrangement is in place to ensure appropriate handling of personal information.

---

39 Confidential, *Submission PR 448,* 11 December 2007. See also Privacy NSW, *Submission PR 468,* 14 December 2007.

40 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556,* 7 January 2008; National Transport Commission, *Submission PR 416,* 7 December 2007.

41 Australian Federal Police, *Submission PR 545,* 24 December 2007.

42 National Transport Commission, *Submission PR 416,* 7 December 2007.

17.31 The ALRC notes stakeholder concerns about the resource implications of drafting an MOU every time an intergovernmental body is involved in the handling of personal information. The ALRC has accommodated these concerns. For example, the development of MOUs should not be a statutory requirement under the *Privacy Act*. Further, the ALRC's recommendation acknowledges that an intergovernmental body may wish to use an arrangement other than a MOU. For example, an intergovernmental body may wish to use a less formal agreement or protocol to ensure appropriate handling of personal information. The ALRC also notes that the Australian Government could develop a template agreement, protocol or MOU for use by various intergovernmental bodies.

17.32 The recommendation is intended to apply to meetings of federal, state and territory officials or intergovernmental bodies that are required to handle personal information. The recommendation could, however, apply equally to intergovernmental bodies that include representatives from foreign governments.

17.33 The ALRC acknowledges stakeholder concerns about how a complaint would be brought against an intergovernmental body. The MOU should outline how an individual can bring a complaint against an intergovernmental body.

17.34 One of the concerns in relation to intergovernmental bodies is that the acts and practices of some state participants may not be regulated by privacy legislation. This issue will be dealt with adequately by recommendations made in this Report—namely that the states and territories enact legislation regulating the handling of personal information in that state or territory's public sector that applies the model UPPs, any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act*. This will ensure that all state and territory participants are subject to privacy regulation and the same privacy principles.

17.35 The ALRC has considered whether the definition of 'agency' under the *Privacy Act* should be amended to cover intergovernmental bodies and COAG created bodies. In the ALRC's view, it would be inappropriate for a federal law to regulate state and territory Ministers and government officials in this way. Such an amendment would intrude too heavily on state and territory governments and may raise constitutional issues. It could be considered to be a law that interferes with the 'existence and nature of a state'.[43]

17.36 The ALRC also has considered whether the definition of 'agency' in the *Privacy Act*, which currently includes a minister, should describe the specific acts and practices of the minister that are covered. In Chapter 41, the ALRC recommends the removal of the political exemption, including the partial exemption that relates to ministers. This will clarify that acts and practices of Australian Government Ministers are regulated by the *Privacy Act* when they are participating in an intergovernmental body.

---

43 *Re Australian Education Union; Ex parte Victoria* (1995) 184 CLR 188, 233; *Austin v Commonwealth* (2003) 215 CLR 185. See discussion in Ch 3.

Recommendation 17–1 When an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies that handle personal information, the Australian Government agency should ensure that a memorandum of understanding or other arrangement is in place to provide for the appropriate handling of personal information.

State and territory regulators

17.37 In Australia there are multiple privacy regulators in particular industry sectors as well as across jurisdictions. As noted in Chapter 14, a number of issues may arise because more than one body is responsible for the regulation of personal information.

17.38 The *Privacy Act* and other federal legislation provide the Privacy Commissioner with a number of powers and functions, including powers to investigate and conciliate complaints, and approve and monitor privacy codes and guidelines.[44] Most states and territories have privacy regulators, but their nature and functions vary widely. For example, New South Wales and Victoria have full-time privacy regulators with a similar range of powers and functions to those of the federal Privacy Commissioner.[45] The Privacy Committee of South Australia's powers and functions, however, are limited compared to the federal, New South Wales and Victorian privacy commissioners.[46] Some jurisdictions, such as Tasmania and the Northern Territory, have regulators with functions other than oversight of the regulation of personal information.[47]

17.39 A number of intergovernmental cooperative schemes employ a single national regulator to enforce compliance with the scheme. For example, the corporations law scheme is enforced by the Australian Securities and Investments Commission, and the gene technology scheme is enforced by the Gene Technology Regulator.

17.40 In DP 72, the ALRC considered whether all formal complaints about privacy should be dealt with by the Privacy Commissioner, rather than by industry ombudsmen and other federal, state and territory regulators. The ALRC also considered whether:

- all formal complaints about privacy under federal legislation could be referred to the Privacy Commissioner; or

---

44 See Part F for a discussion of the powers and functions of the Privacy Commissioner.

45 See discussion in Ch 2.

46 If a person is dissatisfied with the Privacy Committee's response, however, they are referred to the South Australian Ombudsman: see discussion in Ch 2.

47 The Tasmanian Ombudsman regulates privacy in Tasmania. The Northern Territory Information Commissioner is also responsible for overseeing freedom of information and the regulation of public records in the Northern Territory: see discussion in Ch 2.

- the various regimes governing the regulation of privacy at the federal, state and territory levels could be amended to clarify the jurisdiction of each of the bodies that regulate the handling of personal information.

17.41 The ALRC noted that some stakeholders had argued that a single national regulator was desirable to prevent unnecessary costs due to duplication and avoid inconsistencies arising under a national law. Others vigorously opposed a body, such as the OPC, regulating state and territory public sectors.

17.42 The ALRC expressed the preliminary view that there are advantages in having a number of agencies and bodies with responsibility for information privacy. The ALRC proposed, therefore, that the states and territories should enact legislation that regulates the handling of personal information in that state or territory's public sector, and that this legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.[48]

Submissions and consultations

17.43 Only a few submissions addressed this issue. A number of stakeholders supported the retention of state and territory privacy regulators.[49] The Office of the Victorian Privacy Commissioner (OVPC) submitted that maintaining privacy regulators in each jurisdiction fosters greater access to justice by those seeking redress, enables advice to be provided by offices that have developed local expertise, and allows for compliance actions to be undertaken in response to issues and concerns that arise within particular jurisdictions. The OVPC noted that a single national privacy regulator is likely to experience resourcing problems, particularly in relation to complaint handling and education. The OVPC also highlighted that a national privacy regulator would lack expertise in other relevant state and territory laws.[50]

17.44 The Government of South Australia supported the proposal for an independent regulator to be established in South Australia, but noted that the structure of the regulator should be left up to each state and territory.[51]

ALRC's view

17.45 The ALRC has concluded that there are advantages in having a number of agencies and bodies with responsibility for information privacy. These advantages are discussed in Chapter 14, and include: the pooling of resources; peer review and the promotion of high standards in the performance of regulators; the ability of individuals to approach a local regulator for advice and to make a complaint; and the additional expertise that an industry-specific dispute resolution body can provide. The ALRC

---

48 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 4–4.

49 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 518*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

50 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

recommends, therefore, that state and territory privacy legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

17.46 However, the jurisdiction of the various bodies with responsibility for privacy needs to be clarified. Chapter 3 outlines a model for national consistency that seeks to clarify the scope of federal, state and territory information privacy laws. The jurisdiction of the various federal, state and territory bodies with responsibility for information privacy will be clarified once the scheme recommended in this Report is in place.

17.47 There also should be greater cooperation between: the OPC; state and territory privacy regulators; and other bodies with responsibility for information privacy in Australia, such as the Office of the Health Services Commissioner (Victoria) and the Banking and Financial Services Ombudsman. Greater cooperation among regulators will help promote a national and consistent approach to enforcement of privacy laws.

17.48 One method of achieving greater cooperation is the development of MOUs between privacy regulators in relation to enforcement of privacy laws. The ALRC recommends that the OPC develop and publish MOUs with each of the bodies with responsibility for information privacy in Australia, including industry-specific dispute resolution bodies and state and territory bodies with responsibility for privacy.[52] The ALRC notes that the OPC has already entered into a number of MOUs with such bodies, including Privacy NSW.

17.49 To clarify further the jurisdiction of each of the bodies, these MOUs should outline the roles and functions of each of the bodies. They also should outline when a matter will be referred to, or received from, each of the bodies.

17.50 The MOUs should also help to promote consultation between privacy regulators when issuing public interest determinations (PIDs), temporary PIDs, and codes. This will minimise the risk of these instruments introducing inconsistent approaches to the UPPs and any relevant regulations that modify the application of the UPPs. The MOUs should also include a process for the development and publication of joint guidance on the UPPs and any relevant regulations. This will promote a nationally consistent approach to the interpretation of the privacy principles.

17.51 In Chapter 64, the ALRC recommends that the Privacy Commissioner issue one set of rules under the research exceptions to the UPPs to replace the *Guidelines Under Section 95 of the Privacy Act 1988* and the *Guidelines Approved Under Section 95A of the Privacy Act 1988*. The MOUs could also address how the OPC should consult with relevant state and territory bodies when developing these rules.

---

52 The ALRC recommends the development of MOUs to clarify the roles of each of the bodies with responsibility for information privacy in the telecommunications industry: see Ch 73.

Recommendation 17–2 State and territory privacy legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

Recommendation 17–3 The Office of the Privacy Commissioner should develop and publish memorandums of understanding with each of the bodies with responsibility for information privacy in Australia, including state and territory bodies and external dispute resolution bodies with responsibility for privacy. These memorandums of understanding should outline:

(a) the roles and functions of each of the bodies;

(b) when a matter will be referred to, or received from, each of the bodies;

(c) processes for consultation between the bodies when issuing Public Interest Determinations and Temporary Public Interest Determinations, approving codes and developing rules; and

(d) processes for developing and publishing joint guidance.

Privacy rules, codes and guidelines

17.52 In addition to the *Privacy Act* and state and territory legislation, various privacy rules, codes and guidelines regulate the handling of personal information.[53]

17.53 Part IIIAA of the *Privacy Act* allows private sector organisations and industries to develop and enforce their own privacy codes. Once a privacy code has been approved by the Privacy Commissioner, it replaces the NPPs for those organisations bound by the code. The *Privacy Act* requires that these codes contain standards equivalent to those in the NPPs, which would otherwise apply, or to a standard that secures individuals' privacy rights to a higher standard.[54]

17.54 A number of approved privacy codes provide higher standards than those provided in the NPPs. For example, the *Biometrics Institute Privacy Code* provides a number of 'Supplementary Biometrics Institute Privacy Principles' relating to protection, control and accountability.[55] There is no overlap with the NPPs, as a code replaces the NPPs for those organisations bound by it. An organisation, however, may still be subject to other privacy regulation that is inconsistent with these codes. For example, an organisation that provides health services may engage in activities other than those dealt with under the *Biometrics Institute Privacy Code*, and is subject to the *Privacy Act* or a state or territory privacy regime in relation to these activities.

---

53 See Ch 2.

54 *Privacy Act 1988* (Cth) s 16A.

55 Biometrics Institute, *Biometrics Institute Privacy Code—Public Register* (2006) <www.biometricsinstitute.org> at 8 May 2008, 16–18.

17.55 Federal legislation other than the *Privacy Act* also requires the development of privacy guidelines or codes. For example, under s 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth), the Minister may give the Director-General written guidelines to be observed by the Australian Security Intelligence Organisation (ASIO). The Attorney-General has issued a set of guidelines concerning ASIO's functions.[56] The guidelines include rules relating to the treatment of personal information. The guidelines are discussed further in Chapter 37.

17.56 Some state regulatory regimes have adopted provisions from the *Privacy Act*. For example, the Victorian Essential Services Commission has developed *Guideline No 10 (Confidentiality and Informed Consent: Electricity and Gas)* (Guideline No 10). Guideline No 10 requires Victorian electricity and gas retailers to comply with the NPPs whether or not they are 'organisations' under the *Privacy Act* and regardless of when the personal information was collected. Guideline No 10 also protects 'corporate customer information' as personal information. The Law Council of Australia has noted that this is a 'curious provision', given that the High Court of Australia has decided that corporations do not have a right to privacy at common law and that the *Privacy Act* protects the rights of individuals, not corporations.[57]

17.57 The Law Council has also noted that Guideline No 10 requires retailers to apply the NPPs in a narrow way. For example, even if a retailer is providing the same customer with gas and electricity, Guideline No 10 requires the retailer to handle separately customer information about the supply of each service. The Law Council argues that this is a much higher standard than the reasonable expectation test under NPP 2.1(a), and illustrates how the incorporation of NPP-like requirements into state legal regimes can lead to divergence over time.

17.58 Industry organisations have also developed guidelines. Some of these guidelines are not required by legislation. The Australian Direct Marketing Association (ADMA) has developed a *Direct Marketing Code of Practice* that binds ADMA members and all employees, agents, subcontractors and suppliers of ADMA members.[58] The Code includes a schedule that outlines principles to govern fair conduct relevant to consumer data protection.[59] The principles are based on the NPPs and deal with such matters as: limitations on the amount of information that companies can collect about individuals; informing consumers about who is collecting information, and how the company can be contacted; and the intended use of the personal information. Consumers must be

---

56 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 3 April 2008.

57 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. This case is discussed in Ch 74. Law Council of Australia, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act*, 22 December 2004.

58 Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2001), [6]. For further discussion of the Code see Ch 1.

59 Ibid, sch E.

given the opportunity to opt out of future direct marketing approaches and block transfer of their contact details to any other marketer.

Submissions and consultations

17.59 A number of stakeholders noted that if rules, codes and guidelines are not aligned with the *Privacy Act*, they can contribute to inconsistency and fragmentation.[60] The OVPC noted that codes, rules and guidelines can offer less protection than is available under privacy laws where they do not offer individuals a right of complaint or the ability to seek redress for harm suffered.[61] The Australian Retailers Association submitted that a central resource of information on regulatory instruments, including industry codes of practice, should be established and maintained by the OPC.[62]

17.60 Stakeholders also noted, however, that while it is important to limit unnecessary fragmentation of privacy law, additional privacy rules, codes and guidelines can clarify sector-specific issues and provide more detailed protection for personal information where appropriate.[63] The Australian Privacy Foundation submitted that the wide range of privacy rules, codes and guidelines contribute to fragmentation and inconsistency in the regulation of personal information, but noted that with a unified set of privacy principles and greater national consistency there would still be a valuable role for sector or activity specific guidelines and codes.[64]

ALRC's view

17.61 The ALRC acknowledges that privacy rules, codes and guidelines can be beneficial where there is a need for privacy rules to be crafted to the specific needs and practices of particular organisations or industry groups. These documents, however, can contribute to fragmentation and inconsistency of privacy regulation when they are not aligned with existing privacy laws.

17.62 When agencies and organisations are developing privacy rules, codes and guidelines best practice dictates that they should consult with the relevant body responsible for privacy for their industry or sector to ensure that the rules, codes or guidelines will interact and operate effectively with existing privacy laws. Further, agencies and organisations should ensure that the privacy rules, codes and guidelines outline whom an individual can approach with a privacy issue or complaint.

---

60 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; CSIRO, *Submission PR 176*, 6 February 2007; AAMI, *Submission PR 147*, 29 January 2007; Confidential, *Submission PR 143*, 24 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; K Pospisek, *Submission PR 104*, 15 January 2007.

61 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

62 Australian Retailers Association, *Submission PR 131*, 18 January 2007.

63 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

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

Residential tenancy databases

17.63 RTDs raise a range of issues. They are dealt with here because they are currently regulated by inconsistent and fragmented federal, state and territory legislation.

17.64 RTDs are electronic databases operated by private companies containing information about a tenant's rental history. The purpose of such databases is to enable real estate agents to assess 'business risk' on behalf of the property owner. The listings on the database are based on information provided by real estate agents to the database operators. Listings are generally collected from across Australia and access can be obtained nationally.

17.65 In April 2004, the Privacy Commissioner made four determinations concerning a residential tenancy database operator. These determinations included that the operator had breached a number of the NPPs by:

- using an agreement with its members that did not specify sufficiently the data quality standards required;
- failing to take sufficient steps to check listings by property managers and not requiring minimum identification before listing;
- failing to advise tenants contemporaneously that they had been listed;
- using a 'pick list' method of reporting tenancy history, which relied on one category that was broadly defined and on descriptions that were brief, not consistently defined and not mutually exclusive;
- providing an inadequate dispute resolution process;
- failing to provide mechanisms to correct records where the individual concerned had established they were not accurate, complete and up-to-date, or to associate a statement to this effect when there was a dispute about accuracy, completeness or currency;
- charging individuals an excessive amount of money for access via mail to their personal information;
- failing to take reasonable steps to make sure the personal information it collected, used and disclosed was up-to-date; and
- failing to take reasonable steps to destroy or de-identify personal information that was no longer needed for any purpose.[65]

---

65 Office of the Federal Privacy Commissioner, *Complaint Determination No 1 of 2004*, 1 April 2004; Office of the Privacy Commissioner, *Complaint Determination No 2 of 2004*, April 2004; Office of the Privacy Commissioner, *Complaint Determination No 3 of 2004*, April 2004; Office of the Privacy Commissioner, *Complaint Determination No 2 of 2004*, April 2004.

17.66 RTDs contain personal information and so are subject generally to the private sector provisions of the *Privacy Act*. They are also regulated by legislation in some states and territories. The *Privacy Act* currently applies to RTD operators with an annual turnover of $3 million or less, despite the small business exemption, because they trade in personal information.[66] If an RTD operator that is a small business gains consent for the collection or disclosure of an individual's personal information, the *Privacy Act* will not apply.[67] Further, the *Privacy Act* does not contain provisions directed specifically at RTD operators. For example, unlike credit reporting agencies, there is no provision under the *Privacy Act* relating to time limits for the removal of default listings.[68]

17.67 While the states and territories can regulate the actions of the lessors and agents in their jurisdictions, they lack the power to regulate effectively RTD operators based in different jurisdictions.[69] Residential tenancy legislation in New South Wales, Queensland, and now the ACT regulates how real estate agents and lessors list tenants on RTDs.[70] This legislation, however, is incomplete and inconsistent. For example, while the *Property, Stock and Business Agents Regulation 2003* (NSW) provides for the length of time information can be listed,[71] and whether a listed person can access the listing information,[72] the *Residential Tenancies Act 1994* (Qld) does not. In South Australia and the Northern Territory some regulation is provided through fair trading legislation.[73] This is primarily consumer protection legislation, however, and does not relate specifically to RTDs.

17.68 A number of inquiries have now recognised the need for national consistency in the regulation of RTDs.[74] In August 2003, the Ministerial Council on Consumer Affairs (MCCA) agreed with the Standing Committee of Attorneys-General (SCAG) to establish a joint Residential Tenancy Database Working Party. The Working Party released its *Report on Residential Tenancy Databases* on 27 September 2005. The Working Party found that ensuring national uniformity in the treatment of RTDs was essential. It stated, however, that it was inappropriate for the Australian Government to

---

66 See *Privacy Act 1988* (Cth) s 6D(4)(c)–(d); Office of the Privacy Commissioner, *Complaint Determination No 3 of 2004*, April 2004.

67 *Privacy Act 1988* (Cth) s 6D(7), (8).

68 Ibid s 18F.

69 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), [3.2].

70 *Property Stock and Business Agents Regulation 2003* (NSW); *Residential Tenancies Act 1994* (Qld); *Residential Tenancies Act 1997* (ACT).

71 *Property Stock and Business Agents Regulation 2003* (NSW) sch 6A, cl 6(c).

72 Ibid sch 6A, cl 64(a).

73 See, eg, *Fair Trading Act 1987* (SA) pt 4; *Consumer Affairs and Fair Trading Act 1990* (NT) pt 8.

74 Victorian Law Reform Commission, *Residential Tenancy Databases* (2006), [6.5] and rec 1; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 72–73; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

legislate for RTDs and their use by agents, given the existing state and territory responsibilities for agents and tenancy issues.[75]

17.69 The Working Party expressed the view that state and territory legislation should address the relationship between the agent and the tenant. Issues to be addressed include: informing the tenant about the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs. The Working Party recommended that states and territories develop agreed uniform model legislation on the use of RTDs by landlords, agents and listing parties. In April 2006, SCAG agreed to develop model uniform legislation for RTDs. The MCCA has primary responsibility for drafting the legislation.

17.70 The Working Party also concluded that, because the states and territories would generally not be able to regulate directly the operation of RTDs or their interaction with agents, the *Privacy Act* should regulate this aspect of the operation of RTDs. The Working Party was concerned, however, that because the *Privacy Act* does not apply to small businesses that collect or disclose personal with the consent of an individual,[76] RTD operators are not required to comply with other privacy obligations such as those relating to data quality. The Working Party recommended, therefore, that regulations should be made pursuant to s 6E of the *Privacy Act* to prescribe all RTDs as organisations for the purposes of the *Privacy Act*.

17.71 The Working Party also noted that the *Privacy Act* is not prescriptive and does not permit the OPC to direct RTD operators to comply with their obligations under the Act. The Working Party recommended, therefore, that the Australian Government consider the option of a binding code if RTD operators do not comply with the *Privacy Act*.[77]

17.72 In submissions to this Inquiry, stakeholders raised a large number of concerns about the operation of RTDs, including that: tenants are often given little choice when signing tenancy agreements and RTD users routinely extract 'consent' from tenancy applicants; information held on RTDs is sometimes inaccurate;[78] many tenants are unaware that they are listed on an RTD;[79] RTDs can make it difficult for Australian households reliant on the private rental market to secure housing;[80] inconsistent state

---

75 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

76 See *Privacy Act 1988* (Cth) s 6D(7) and (8).

77 As recommended by the Privacy Commissioner in Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 16. Binding codes are considered in Ch 48.

78 Tenants Union of NSW Co-op Ltd, *Submission PR 169*, 5 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007; Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

79 Tenants Union of Victoria Ltd, *Submission PR 197*, 16 February 2007.

80 Ibid; Anglicare Tasmania, *Submission PR 135*, 19 January 2007.

and territory legislation regulating RTDs causes a number of problems;[81] and in some jurisdictions there is no body to receive complaints about RTDs.[82]

17.73 In DP 72, the ALRC agreed with the recommendations of the RTD Working Party that the states and territories should enact legislation that addresses the relationship between the agent and the tenant, including issues such as: informing the tenant about the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs. The OPC and the OVPC endorsed uniform state and territory legislation to regulate the use of RTDs by landlords, agents and other listing parties.[83]

17.74 The ALRC also expressed the view that all RTD operators should be regulated by the *Privacy Act*, regardless of whether they are small business operators or whether they gain consent for the collection or disclosure of an individual's personal information. The ALRC noted that the then Attorney-General had announced that regulations to extend the coverage of the *Privacy Act* to all RTDs were complete.

17.75 The ALRC noted that some stakeholders had argued that all RTD operators should be brought under the *Privacy Act* and that the OPC should make a binding code in relation to them.[84] Others supported both state and territory legislation and a binding code under the *Privacy Act*.[85] One stakeholder submitted that it did not believe that the need for a binding code on RTD operators had yet been demonstrated, but that it may be supportive in the future if this is required.[86]

17.76 The ALRC did not propose the making of a binding code to regulate RTD operators. It was the ALRC's view that state and territory legislation regulating the use of RTDs and the regulation of RTD operators by the *Privacy Act* should deal with many of the issues identified in the submissions. The ALRC also expressed the view that it would be appropriate for the Privacy Commissioner to delegate his or her complaint-handling powers in relation to RTD operators to state and territory tenancy tribunals and equivalent bodies.

---

81 Tenants Union of Victoria Ltd, *Submission PR 197*, 16 February 2007; Anglicare Tasmania, *Submission PR 135*, 19 January 2007. See also R Harrison and D Imber, 'Residential Tenancy Databases: Need for National Regulation' (2007) 3(8) *Privacy Law Bulletin* 98.

82 Anglicare Tasmania, *Submission PR 135*, 19 January 2007.

83 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

84 Queensland Government, *Submission PR 242*, 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Legal Aid Queensland, *Submission PR 212*, 27 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; Anglicare Tasmania, *Submission PR 135*, 19 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.

85 See, eg, Tenants Union of NSW Co-op Ltd, *Submission PR 169*, 5 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007.

86 Real Estate Institute of Australia, *Submission PR 84*, 12 January 2007.

Submissions and consultations

17.77 Some stakeholders continued to raise concerns about the operation of RTDs.[87] Anglicare submitted that the Privacy Commissioner should develop and enforce a binding code that provides detailed guidance on compliance with the *Privacy Act* by RTD operators and their customers.[88] The Australasian Compliance Institute indicated that it supported the Privacy Commissioner imposing further requirements on RTD operators in the future if there was evidence of 'privacy problems'.[89]

17.78 The Queensland Government addressed the ALRC's view that the Privacy Commissioner could delegate his or her complaint-handling powers in relation to RTD operators to state and territory tenancy tribunals and equivalent bodies. It submitted that:

> consultation on the detail of how such a proposal would be implemented, and to determine capacity and resourcing, must occur with tenancy authorities and counterpart complaints tribunals (in Queensland, the Small Claims Tribunal). … Additionally, the Queensland Government notes that this proposal may give rise to confusing duplication, with tenancy-related privacy complaints handled by tenancy dispute authorities and general privacy complaints by existing dedicated privacy regulators or complaint frameworks.[90]

ALRC's view

17.79 A number of reviews have established the need for stronger and nationally consistent regulation of RTDs. The ALRC shares the concerns raised in these reviews and of those who made submissions to this Inquiry in relation to the collection, use and disclosure of personal information held on RTDs. The ALRC agrees with the recommendations of the RTD Working Party that states and territories should enact legislation that addresses the relationship between the agent and the tenant. Legislation would address issues such as: informing the tenant about the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs. The ALRC notes that the MCCA is in the process of developing raft legislation.

17.80 Further, all RTD operators should be regulated by the *Privacy Act* regardless of whether they are small business operators. In this regard, the ALRC notes the promulgation of the *Privacy (Private Sector) Amendment Regulations 2007 (No 3)* (Cth). The Regulations amend the *Privacy (Private Sector) Regulations 2001* (Cth) to provide that under s 6E(2) of the *Privacy Act* a small business which operates a residential tenancy database and undertakes certain acts and practices is prescribed as an organisation.

---

87 Confidential, *Submission PR 535,* 21 December 2007; Anglicare Tasmania, *Submission PR 514,* 21 December 2007; R Lucienne, *Submission PR 477,* 16 December 2007.

88 Anglicare Tasmania, *Submission PR 514,* 21 December 2007.

89 Australasian Compliance Institute, *Submission PR 419,* 7 December 2007.

90 Queensland Government, *Submission PR 490,* 19 December 2007.

17.81 The ALRC does not recommend the making of binding rules to regulate RTD operators. It is the ALRC's view that state and territory legislation regulating the use of RTDs and the regulation of RTD operators by the *Privacy Act* should deal with many of the issues identified in submissions.

17.82 As noted in Chapter 48, the ALRC is no longer of the view that the *Privacy Act* should be amended to empower the Privacy Commissioner to develop and impose a binding code. The ALRC notes, however, that the Privacy Commissioner could request that RTD operators develop a privacy code to be approved by the Privacy Commissioner under Part IIIAA of the *Privacy Act*. Alternatively, the Minister could make regulations under the Act to regulate RTDs. In the ALRC's view, the OPC should monitor the use and operation of RTDs in order to determine whether it should request that RTD operators develop a privacy code, or that it should advise the Minister to make regulations under the *Privacy Act* to regulate RTD operators.

17.83 The ALRC notes stakeholder concerns that tenants with privacy complaints about the handling of personal information by RTD operators should be able to have those complaints dealt with by a state or territory tenancy tribunal or an equivalent body. These bodies are well suited to deal with privacy matters in the residential tenancy context—they are quick, accessible and affordable.

17.84 In Chapter 49, the ALRC recommends that the *Privacy Act* be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of his or her powers in relation to complaint handling. In the ALRC's view, it would be appropriate for the Privacy Commissioner to delegate his or her complaint-handling powers in relation to RTD operators to state and territory tenancy tribunals and equivalent bodies under this section.

17.85 The ALRC acknowledges, however, the concerns of the Queensland Government. In the ALRC's view, the Privacy Commissioner should consult with relevant state and territory tenancy tribunals before making such a delegation. Further, any confusion or duplication relating to the handling of complaints about RTDs would be ameliorated by clear delegations of power, the development of MOUs between the OPC and relevant state and territory tenancy tribunals,[91] and community education.

91 See Recommendation 17–3.

Part D

The Privacy Principles

18. Structural Reform of the Privacy Principles

Contents

Introduction to Part D

18.1 Part D of this Report recommends reforming the privacy principles in the *Privacy Act 1988* (Cth). Currently, the Act contains two sets of privacy principles: the Information Privacy Principles (IPPs),[1] which apply to public sector 'agencies'; and the National Privacy Principles (NPPs),[2] which apply to private sector 'organisations'.[3] Both sets of privacy principles regulate the handling of personal information. They do not cover other areas of privacy such as bodily privacy, surveillance, or communications privacy.

1 See *Privacy Act 1988* (Cth) s 14.
2 See Ibid sch 3.
3 The terms 'agency' and 'organisation' are defined, respectively, in Ibid ss 6(1) and 6C.

18.2 In this Part, the ALRC recommends reforming the existing privacy principles in two main ways: first, by consolidating the IPPs and NPPs; and secondly, by amending, where warranted, the substantive content of the privacy principles.

18.3 This chapter considers reform to the structure of the privacy principles. It explains how the IPPs and NPPs currently operate and recommends the creation of a single, unified set of privacy principles, to apply across the public and private sectors.

18.4 For convenience, this Report refers to the recommended single set of privacy principles as the Unified Privacy Principles (UPPs), a term used to reflect the fact that they are largely the product of unifying the NPPs and IPPs. Upon the implementation of the ALRC's recommendation to adopt a single set of principles in the *Privacy Act*, it is likely that a different term will be used to describe the privacy principles.

18.5 The ALRC has drafted model UPPs for the purposes of this Report.[4] These model UPPs are merely indicative of how the privacy principles in the Act may appear if the ALRC's relevant recommendations were to be implemented. The ALRC anticipates that, if its recommendations are accepted, the Australian Government will instruct the Office of Parliamentary Counsel to draft the new privacy principles using the ALRC's recommendations as a template, rather than simply adopting the ALRC's model UPPs in their current form.

18.6 The remaining chapters in Part D recommend reform to the substantive content of the privacy principles. They proceed largely on the assumption that the ALRC's recommendations in this chapter will be implemented. Nevertheless, even if some or all of the recommendations in this chapter are not implemented, the other recommendations in this Part remain applicable insofar as they focus on reform to the substantive requirements of the Act's two existing sets of privacy principles, the IPPs and NPPs.

18.7 In this Part, the ALRC analyses privacy thematically. In relation to each aspect of the principles there is a brief explanation of how the IPPs and NPPs currently apply and a summary of any relevant issues relating to their operation. This is followed by the ALRC's recommendations for reforming the applicable privacy principle or, where relevant, for the provision of specific guidance by the Office of the Privacy Commissioner (OPC).

Development of current Australian privacy principles

OECD Guidelines

18.8 The preamble to the *Privacy Act* notes that Australia is a member of the Organisation for Economic Co-operation and Development (OECD); that the Council of the OECD has recommended that member countries take into account in their

4 The model UPPs are set out in full at the beginning of this Report. They are also reproduced individually in relevant chapters in this Part.

domestic legislation the privacy principles set out in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines); and that Australia has expressed its intention to participate in the recommendation. The privacy principles in the OECD Guidelines, which apply to personal data in both the public and private sectors, are the foundation for the two sets of privacy principles in the *Privacy Act*: the IPPs and the NPPs.

18.9 The OECD Guidelines were adopted by the OECD Council on 23 September 1980. They were designed to discourage the member countries of the OECD from introducing 'incompatible and conflicting laws for the defence of privacy in the newly established databases of the interlinked information technologies'.[5] As such, the OECD Guidelines have influenced data protection laws in many jurisdictions.

18.10 The OECD Guidelines attempt to reconcile sometimes competing interests. The goal of protecting privacy and individual liberties is balanced with the desire to advance the free flow of personal information.[6] The Guidelines were developed to harmonise national privacy legislation and, while upholding human rights, simultaneously to prevent interruptions in the cross-border flow of information.[7]

18.11 The OECD Guidelines 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'.[8] On one hand, they are 'minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties'.[9] On the other hand, the OECD Guidelines deter member countries from creating unnecessary obstacles to cross-border flows of personal information in the name of the protection of privacy and individual liberties.[10]

18.12 Part Two of the OECD Guidelines sets out eight basic information privacy principles: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability.[11] Most of these principles are reflected explicitly in the IPPs and the NPPs. Although there is no principle in the IPPs or NPPs called 'Accountability', aspects of the accountability

---

5 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 25.

6 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [25].

7 Ibid, preface.

8 Ibid, Guideline 2.

9 Ibid, Guideline 6.

10 Ibid, Guideline 18.

11 See Ibid, Guidelines 7–14. The OECD Guidelines are set out in Ch 1.

principle are incorporated in other provisions in the *Privacy Act*, such as those dealing with investigations of complaints regarding privacy breaches.[12]

18.13 A critical question, faced both by the drafters of the OECD Guidelines and member states seeking to implement the Guidelines, is: what should be set out in general privacy principles and what should be set out in more detailed provisions? The Explanatory Memorandum to the OECD Guidelines states:

> The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions … should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a dividing line between the level of basic principles or objectives and lower level 'machinery' questions which should be left to domestic implementation.[13]

18.14 John Gaudin has expressed the view that the OECD Guidelines are grounded in the society, technology and culture of the 1970s and that the principles in the Guidelines are insufficiently flexible to accommodate the extensive changes that have taken place since they were promulgated.[14] He has stated that the OECD Guidelines reflect assumptions about the future development of information technology, which are now seen to be limited.[15] Justice Michael Kirby, who chaired the OECD Expert Group on Privacy, has stated extrajudicially:

> There appears to be a need to review the 1980 OECD Guidelines, which are already showing signs of their age. Informed writers are already suggesting the necessity for privacy principles apt to contemporary technology … Clearly the 'openness principle' of the OECD Guidelines was always one of the weakest. The advent and potential of the internet require that there be new attention to it.[16]

18.15 In addition to the OECD Guidelines, on 26 November 1992, the Council of the OECD adopted the *Guidelines for the Security of Information Systems*. These further Guidelines aimed 'to raise awareness of risks to information systems and of the safeguards available to meet those risks', and 'to create a framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems'.[17] Due to the dramatic change in the information technology environment

---

12 See Part F of this Report, which discusses data breach and the powers of the OPC.

13 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19 (e)]. See also [50].

14 J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part II' (1997) 3 *Privacy Law & Policy Reporter* 196, 199.

15 See J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part I' (1996) 3 *Privacy Law & Policy Reporter* 143, 144.

16 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 27. The question whether the *Privacy Act* should be technology neutral is addressed in Ch 10.

17 See Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems* (1992).

since 1992, those Guidelines were replaced by the OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, which were adopted on 25 July 2002 (the OECD Security Guidelines).

18.16 The OECD Security Guidelines contain nine information systems security principles entitled: awareness; responsibility; response; ethics; democracy; risk assessment; security design and implementation; security management; and reassessment. The awareness principle provides that 'participants should be aware of the need for security of information systems and networks and what they can do to enhance security'[18] and the response principle provides that 'participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents'.[19]

Information Privacy Principles

18.17 Section 14 of the *Privacy Act* contains 11 IPPs. The IPPs were included in 1988, in the original version of Act, and have not been amended since that time. Until 2000, the IPPs were the only privacy principles in the Act.

18.18 The IPPs regulate the collection, storage, use and disclosure of an individual's personal information, and provide for individuals to access and correct their personal information. The IPPs apply to personal information handled by Commonwealth and ACT government agencies.[20]

18.19 The Privacy Commissioner has issued a series of guidelines on the interpretation of the IPPs.[21] The guidelines note that:

> The IPPs set out minimum standards for agencies. Compliance with the IPPs is a legal obligation, but minimal compliance will not always be an appropriate approach for an agency to take … Especially where sensitive information is concerned, or where mishandling of personal information may have serious consequences, more care to protect individuals' privacy may be appropriate than is required by the letter of the IPPs.[22]

---

18 Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002), Principle 1.

19 Ibid, Principle 3.

20 See *Privacy Act 1988* (Cth) ss 13(a), 16. The definition of 'agency' in *Privacy Act 1988* (Cth) s 6(1) includes: a minister; a Department; a body established for a public purpose; a federal court; and the Australian Federal Police. This definition is also discussed in Ch 5.

21 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994); 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). The status of guidelines is discussed in Part F of this Report.

22 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).

National Privacy Principles

18.20 Schedule 3 to the *Privacy Act* contains 10 further privacy principles, the NPPs. Schedule 3 was not part of the original Act. It was introduced by the *Privacy Amendment (Private Sector) Act 2000* (Cth).

18.21 The NPPs apply generally to private sector 'organisations', unless the organisation in question is subject to an approved privacy code.[23] The term 'organisation' is defined in s 6C as an individual, a body corporate, a partnership, any other unincorporated association or a trust. This definition is subject to a number of qualifications, however, exempting, among others: individuals acting in a personal capacity; small business operators; political parties; government agencies; and state or territory authorities and prescribed instrumentalities.[24]

18.22 The NPPs regulate the following aspects of the handling and management of personal information: collection; use and disclosure; data quality; data security; openness of data management policies; individuals' rights of access to and correction of their personal information; the use of identifiers; individuals' right to maintain their anonymity; transborder data flows; and how sensitive information should be treated.

18.23 The stated objectives of the NPP regime are:

> (a) to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations; and
>
> (b) to do so in a way that:
>
> (i) meets international concerns and Australia's international obligations relating to privacy; and
>
> (ii) recognises individuals' interests in protecting their privacy; and
>
> (iii) recognises 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 right of business to achieve its objectives efficiently.[25]

Principles-based regulation

18.24 The NPPs and IPPs—together referred to as the privacy principles—represent the main regulatory mechanism in the *Privacy Act*. Parliament deemed it preferable to regulate privacy using, for the most part, broad principles, as distinct from using a

---

23 *Privacy Act 1988* (Cth) s 16A. See also the relevant Second Reading Speech: Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15749–15750. Privacy codes are discussed in Part F of this Report.

24 The private sector exemptions to the *Privacy Act* are discussed in Part E of this Report.

25 *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3.

more conventional method of detailed, prescriptive regulation—sometimes referred to as 'rules-based regulation'.[26]

18.25 In Chapter 4, the ALRC expresses the view that principles-based regulation should be the primary method used to regulate information privacy in Australia. Importantly, however, the ALRC does not recommend the adoption of a pure form of principles-based regulation, recognising the benefits of allowing principles to be supplemented by more specific rules in regulations or other legislative instruments, in order to accommodate different industries or policy considerations. In later chapters, this Report addresses detailed regulation in certain specific areas—namely health and research,[27] credit reporting[28] and telecommunications.[29]

18.26 In addition, a primarily principles-based framework can itself adopt varying degrees of detail and prescription within its principles. The IPPs and NPPs each contain detailed rules and high-level principles. For example, NPP 2 sets out relatively detailed rules related to the use and disclosure of personal information, whereas NPP 3 provides a broad, high-level principle relating to data quality.

18.27 Professor Julia Black suggests three broad categories of regulatory method: 'bright line' rules; 'principles' and 'complex or detailed rules'.[30] Table 18.1 below provides hypothetical examples of each of these three types of regulatory method. The paragraphs immediately following it explain how these different forms of regulation operate.[31]

Table 18.1: Hypothetical examples of regulatory methods

Bright line rule	Principle	Complex/detailed rule
An organisation must not collect personal information relating to an individual's sexuality.	An organisation must not collect personal information unless it is necessary for one of its functions or activities.	An organisation [defined] must not collect [defined] personal information [defined] unless all of the following conditions are met: [list of conditions].

26 Ch 4 provides an overview of regulatory theory and the different forms of regulation. In particular, it generally compares principles-based and rules-based regulation.

27 See Part H.

28 See Part G.

29 See Part J.

30 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 10. There are, of course, many other ways of differentiating between the various methods of regulation. See, eg, R Baldwin, *Rules and Government* (1995), 7–11.

31 This part of the chapter is adapted from J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 10.

18.28 As Table 18.1 illustrates, a 'bright line' rule contains a single criterion of applicability. Such rules are clear and straightforward to apply, but can fail to achieve their goal because there is considerable scope for manipulation or creative compliance. For instance, the rule may not be broad enough to capture all of the conduct that it is intended to proscribe, or an organisation may seek a loophole so as to comply with the letter, but not the spirit, of the rule.

18.29 A 'principle' articulates substantive objectives. Whether a principle is certain depends on whether there is general consensus about what is required to achieve compliance. While principles may appear simple to apply—in that they are concise and avoid arcane language—problems can arise in practice where, for instance, there is a dispute as to the meaning of the key terms. In the example from Table 18.1 above, reasonable minds may differ over what is necessary, in a particular context, for an organisation's functions or activities.

18.30 A complex or detailed rule can provide a higher degree of certainty because it expressly lists the relevant conditions to be taken into account. Applying such a rule, however, is complex, and the creation of a list of conditions inevitably will leave gaps resulting in scope for manipulation or creative compliance.

18.31 The discussion below considers the level of detail and prescription that ought to be embodied within the privacy principles.

Level of detail, guidance and protection

Background

18.32 Existing models of privacy principles vary in the level of detail and guidance that they provide. For example, the OECD Guidelines are pitched at a high level—they are relatively broad and aspirational—while the Victorian health privacy principles are considerably more detailed and comprehensive.[32]

18.33 An advantage of high-level principles is that they allow for greater flexibility. They can more easily accommodate unforeseen circumstances and a changing technological environment. For example, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework states that the high-level nature of the OECD Guidelines 'makes them still relevant today'.[33]

18.34 A disadvantage of high-level principles, however, is that they can fail to provide adequate guidance. In turn, this may promote a proliferation of guidelines and information sheets, which may not be legally binding. In contrast, detailed rules provide more guidance, thereby promoting certainty and consistency in application.

---

32 *Health Records Act 2001* (Vic) sch 1.

33 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), fn 1.

18.35 The choice about how prescriptive the principles should be also reflects, to some degree, a wider policy choice about the degree to which the regulation of personal information should be 'light-touch'. The private sector provisions of the *Privacy Act* introduced what the then Attorney-General described as a 'light-touch' co-regulatory approach to information privacy protection, which was intended to be responsive to business and consumer needs.[34] This was to be achieved, in part, by adopting high-level principles rather than prescriptive rules.[35] It is generally more difficult to establish a breach of high-level principles than provisions imposing detailed and specific obligations.

18.36 Another issue is whether the privacy principles should contain a minimum, intermediate or maximum level of protection of personal information. Commentators have noted that there is a choice between two broad dynamics in modelling privacy principles in a globalised environment:

> On the one hand, countries [could] progressively fashion their privacy protection policies according to the highest standard, a 'trading up' or a 'race to the top'. Conversely, countries might consider that a less-regulated climate would attract global business that would want to circumvent the higher standards at work elsewhere. This competitive deregulation would lead to a race to the bottom, as countries progressively weaken their standards to attract global investment in the information technology and services industries.[36]

Submissions and consultations

Level of detail

18.37 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked:

> Should federal privacy principles be prescriptive or should they provide high level guidance only? Should they aim for a minimum or maximum level of protection of personal information or aim to adopt a best practice approach?[37]

18.38 In response to IP 31, a very large number of stakeholders favoured privacy principles that provide high-level guidance, as distinct from those prescribing in detail what is and is not permissible.[38] Stakeholders submitted that such an approach permits

---

34 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General).

35 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 164.

36 C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), xv.

37 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–36.

38 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Queensland Government, *Submission PR 242*, 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; National

greater flexibility;[39] and, by emphasising the objectives of the law rather than its detail, promotes technological neutrality and makes the law more resilient to change.[40] The OPC submitted that this also aids in ensuring the law is clear and easy to apply.[41]

18.39 Further, it was argued that principles-based regulation is more appropriate in a co-regulatory environment.[42] For example, the OPC submitted:

> Principle-based law is aimed at encouraging organisations to understand the values behind the law and change their behaviour accordingly; not just to prevent action from being taken against them by a regulator, but because they understand why the law is there, what its objectives are and that it may benefit its business outcomes.[43]

18.40 The Australian Government Department of Employment and Workplace Relations submitted that using language that is not overly prescriptive will make it easier to move to a unified set of privacy principles, applicable to the public and private sectors.[44]

18.41 Some stakeholders, however, suggested that a balance should be struck between high-level guidance and the more detailed prescription associated with traditional legislative regulation.[45] Others suggested that it is necessary to adopt a more prescriptive approach. Professor William Caelli submitted:

> Privacy Principles MUST be prescriptive or else they will be largely ignored … There is no evidence that the private or public sector alike have embraced advanced information security systems WITHOUT legal obligation. This could also be clearly

---

Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; AXA, *Submission PR 119*, 15 January 2007; Microsoft Australia, *Submission PR 113*, 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; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85*, 12 January 2007.

39 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85*, 12 January 2007.

40 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

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

42 Ibid; Law Council of Australia, *Submission PR 177*, 8 February 2007; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

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

44 Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 2007.

45 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; AAMI, *Submission PR 147*, 29 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

> stated even for many matters of safety, eg, seat belts being made compulsory for inclusion in any manufactured or imported car, etc.[46]

18.42 In the Discussion Paper, *Review of Australian Privacy Laws* (DP 72), the ALRC proposed that the:

(a) obligations in the privacy principles generally should be expressed as high-level principles;

(b) privacy principles should be simple, clear and easy to understand and apply; and

(c) privacy principles should impose reasonable obligations on agencies and organisations.[47]

18.43 This proposal received general support from a majority of stakeholders.[48] Stakeholders expressed the view that a high-level principle approach works well in practice, and emphasised the adaptability and flexibility of such an approach.[49] It was also noted that a prescriptive approach would increase compliance costs.[50] Optus noted:

> Optus fully supports the high level principle approach to specifying obligations via the use of the privacy principles. In practice, this approach works well, and has provided the necessary guidance to organisations when creating privacy safeguards for a multitude of different circumstances and emerging technologies.[51]

---

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

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 15–1. Submissions and consultations on limb (c) of the proposal are addressed separately below.

48 BPay, *Submission PR 566*, 31 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 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; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Queensland Government, *Submission PR 490*, 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; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; National Transport Commission, *Submission PR 416*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 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.

49 See, eg, Optus, *Submission PR 532*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; National Transport Commission, *Submission PR 416*, 7 December 2007.

50 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

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

18.44 Similarly, Microsoft Asia Pacific submitted that

> a principles based approach to regulation allows for the achievement of regulatory objectives while giving regulated entities the flexibility to determine how to do so. Principles based regulation is also more robust and adaptable to changing information handling practices.[52]

18.45 Medicare Australia stated:

> (a) We agree that high level principles are preferable to a more rigid detailed-rule regime, given the vast array of circumstances and contexts they will apply to. A detailed-rule regime would result in long, complex instructions because they would need to cover off all possible permutations of interactions. By setting the principles to express desired outcomes rather than prescribed processes, this allows particular agencies and organisations the flexibility to implement their processes to meet the objectives of the principles in the most appropriate way for their environments …
>
> (b) It will be vital that the principles [be] … simple, clear, easy to understand and … apply to avoid ambiguity and the risk that they will be interpreted widely differently. This will provide confidence that they will be applied in a consistent manner.[53]

18.46 Privacy advocates generally supported the proposal, and submitted that it was desirable to adopt principles which also are consistent within Australia, and represent best practice in internationally accepted privacy standards.[54]

18.47 Some stakeholders that supported a high-level principle approach also expressed the need for some level of prescription, where necessary. For example, the Social Security Appeals Tribunal (SSAT) recognised the importance of providing greater precision and certainty in particular instances, such as those covered in NPP 2 regulating use and disclosure of personal information. It expressed the view that the current hybrid regulatory model underpinning privacy protection should be maintained.[55] The Public Interest Advocacy Centre (PIAC) submitted that there needs to be guidance about how high-level principles operate, and that such guidance ideally should be contained in the *Privacy Act* in the form of more prescriptive provisions.[56]

18.48 Liberty Victoria opposed outright the approach proposed in DP 72, and submitted that privacy principles should be prescriptive and detailed. It stated that:

> We believe that the starting point for protection of privacy is recognising that people have a human right to privacy, rather than considerations about burdening the private or public sectors. The intrusive technology available today and likely to be more

---

52 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.
53 Medicare Australia, *Submission PR 534*, 21 December 2007.
54 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
55 Social Security Appeals Tribunal, *Submission PR 478*, 17 December 2007.
56 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007

sophisticated in the future demands a more stringent rather than light-touch approach to privacy protection.[57]

Minimum standards or maximum protection?

18.49 In response to IP 31, a number of stakeholders submitted that the privacy principles should continue to articulate minimum standards, as distinct from attempting to provide maximum privacy protection.[58] Some stakeholders linked this with the intention to adopt a 'light-touch' regulatory approach.[59] The Australian Bankers' Association argued that the current approach is working well and that those who favour more onerous regulation should first be required to 'establish the case for additional regulation and to demonstrate the benefits'.[60] It was also noted that the imposition of more onerous obligations would strengthen arguments for retaining an exemption for small businesses in the *Privacy Act*.[61]

18.50 While acknowledging the importance of having privacy principles, a number of stakeholders noted that this does not preclude some aspects of privacy from being regulated in a more prescriptive manner, where this is required by the particular situation.[62] The OPC observed that the NPPs and IPPs were always intended to be 'minimum standards' that ought properly to be supplemented in appropriate circumstances.[63] Similarly, other stakeholders observed that the current approach whereby the IPPs and NPPs are supplemented by codes of practice and other guidance operates effectively.[64]

---

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

58 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

59 Veda Advantage, *Submission PR 163,* 31 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

60 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007. See also Government of South Australia, *Submission PR 187,* 12 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

61 Government of South Australia, *Submission PR 187,* 12 February 2007. The exemptions in the *Privacy Act* are discussed in Part E.

62 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.

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

64 Veda Advantage, *Submission PR 163,* 31 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

18.51 As noted above, the ALRC in DP 72 proposed that an objective to be pursued in drafting the privacy principles in the *Privacy Act* should be to impose reasonable obligations on agencies and organisations.[65] This approach was generally supported.[66]

18.52 PIAC expressed some concern about the drafting of the proposed objective because of uncertainty concerning the meaning of 'reasonable'. It submitted that:

> The word 'reasonable' is open to many different interpretations. What is 'reasonable' from a business perspective may be very unreasonable from a consumer perspective. PIAC would prefer the following wording: 'the privacy principles should impose reasonable obligations on agencies and organisations *that effectively protect the privacy interests of individuals*'.[67]

18.53 Medicare Australia stated that it assumed the term 'reasonable obligations' would be interpreted as meaning obligations that are reasonable in the circumstances, and that guidance on this would be useful.[68]

18.54 The Office of the Victorian Privacy Commissioner expressed the view that 'obligations placed on agencies and organisations should be of the highest possible standard that is reasonable and practicable'.[69] In contrast, the SSAT preferred that the principles continue to reflect a minimum level of privacy protection.[70]

ALRC's view

Level of detail

18.55 A principles-based approach should continue to be at the heart of the *Privacy Act*, and this should remain the starting point for the regulation of privacy. The ALRC favours such an approach because it is more flexible and able to adapt to the multitude of circumstances in which agencies and organisations must take account of individuals' privacy rights. These features make the *Privacy Act* more resilient to change, especially in response to technological developments that impact on privacy. Further, the privacy principles, as far as practicable, should be drafted in technology-neutral terms.[71] This is

---

65 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 15–1(c).

66 BPay, *Submission PR 566*, 31 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; 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; Centre for Law and Genetics, *Submission PR 497*, 20 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; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; National Health and Medical Research Council, *Submission PR 397*, 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.

67 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007 (emphasis added).

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

69 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

70 Social Security Appeals Tribunal, *Submission PR 478*, 17 December 2007.

71 The merits of technology-neutral principles are discussed in Ch 10.

the best way to ensure that the principles can continue to be relevant in the face of technological change.

18.56 It must be stressed, however, that the IPPs and NPPs are not constituted exclusively by archetypal high-level principles. Some of the principles such as IPP 9 (Personal information to be used only for relevant purposes) and NPP 8 (Anonymity) are relatively brief, expressing broad and general obligations or objectives to be achieved. On the other hand, principles such as IPP 5 (Information relating to records kept by record-keeper) and NPP 2 (Use and disclosure) are more detailed, specifying with greater precision the obligations that apply in the relevant circumstances. In other words, the IPPs and NPPs represent a compromise.

18.57 A compromise or hybrid approach is desirable because it enables Parliament to respond more flexibly to the needs of individuals, agencies and organisations at the various stages of the information cycle. Relying solely on either rules-based or principles-based regulation would not provide agencies and organisations with sufficient flexibility or certainty in the application of the principles.

18.58 Commentators have noted that an advantage of a hybrid system is that it seeks to take the advantages of both a principles-based and a rules-based system in order to achieve regulatory clarity, enforceability and flexibility.[72] The continuation of a hybrid regulatory scheme will allow agencies and organisations to understand the purpose of the law and to drive organisational behaviour towards best practice. It therefore strikes an appropriate balance between flexibility and certainty. The overall regulatory structure should provide more detailed guidance and regulation where it is necessary to deal with particular issues.

18.59 The ALRC therefore recommends that the obligations in the privacy principles generally should be expressed as high-level principles. This should remain a broad objective, rather than a strict rule, in the drafting of the privacy principles. As demonstrated by the ALRC's approach in determining the content of the UPPs, some principles—such as anonymity and pseudonymity, collection, and data quality—contain high-level obligations; whereas others—such as use and disclosure, and access and correction—are more prescriptive.

18.60 The privacy principles should also be drafted with the objective of making them simple, clear and easy to understand and apply.

18.61 The ALRC notes the view expressed in submissions that the privacy principles should be consistent within Australia. This view is accommodated within

---

72 O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 332.

recommendations in Chapter 3 of this Report dealing with national consistency, as well as the recommendation that one of the objects of the *Privacy Act* should be 'to provide the basis for nationally consistent regulation of privacy and the handling of personal information'.[73]

Minimum standards or maximum protection?

18.62 The ALRC affirms the longstanding policy position that the *Privacy Act* should be light-touch, in the sense that it should provide only such regulation as is required to protect individuals' privacy without unreasonably burdening the public or private sectors. To further this goal, the privacy principles should impose reasonable obligations on agencies and organisations that provide adequate protection of individuals' privacy rights and help to promote best practice, without creating an excessive compliance burden.

18.63 Determining whether an obligation is reasonable will involve a consideration of the impact of imposing the obligation on all the participants in the regulatory regime, including the agencies and organisations that are regulated, and the individuals intended to benefit from that regulation. Assessments of whether obligations are reasonable invariably require consideration, and often a balancing, of many factors. These factors include the privacy protection that will be afforded to individuals by imposing the obligation, the compliance burden, and the need to ensure that agencies and organisations can exercise properly their lawful functions while complying with the obligation. A consideration and balancing of such factors may result in a principle which allows for specified exceptions to an obligation or which provides that an obligation arises only where it is reasonable and practicable in the circumstances.

18.64 The benefits and costs of privacy protection to society as a whole are also relevant considerations in framing privacy principles. Professor Fred Cate has stated that:

> Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and individual privacy have value and are necessary in a democratic society and market economy. That value benefits individuals as well as society as a whole. Therefore, the goal of any privacy regime must be to balance the value of accessible personal information with the value of information privacy to maximize both individual and public benefits.[74]

---

73 See Rec 5–4. The ALRC has also recommended that one of the objects of the *Privacy Act* should be to implement, in part, Australia's obligations at international law in relation to privacy. This accommodates, to some extent, the view expressed by some that the privacy principles should represent best practice in internationally accepted privacy standards: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

74 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341, 369.

18.65 By stipulating that the obligations to be imposed on agencies and organisations are to be reasonable, it is unnecessary to recommend obligations in every privacy principle that uniformly represent either minimum or maximum levels of protection. The ALRC's approach in this regard is consistent with a hybrid regulatory approach, and with the goal of maintaining flexibility. In certain areas, it may be necessary to provide more detailed regulation that imposes either stricter or more lenient obligations.[75] In some situations, the obligations in the privacy principles will be displaced by more specific obligations that apply in a particular area—for instance, in credit reporting, health services and research, and in the telecommunications industry.[76]

Recommendation 18–1 The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:

(a) the obligations in the privacy principles generally should be expressed as high-level principles;

(b) the privacy principles should be technology neutral;

(c) the privacy principles should be simple, clear and easy to understand and apply; and

(d) the privacy principles should impose reasonable obligations on agencies and organisations.

Towards a single set of privacy principles

Background

18.66 The ALRC considered whether it is preferable to maintain two separate sets of similar, but sometimes inconsistent, privacy principles, or to create a unified set of privacy principles.[77]

18.67 The existence of two sets of privacy principles may cause difficulties for agencies and organisations seeking to comply with the *Privacy Act*. There are circumstances when an organisation or agency is subject to both the IPPs and the NPPs. For example, an Australian Government contractor may be bound under the Act

75 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 12.

76 For those more detailed requirements, see Parts G, H and J of this Report.

77 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–34.

to comply with the NPPs but also may be bound by contract to comply with the IPPs.[78] Some government business enterprises—such as Australia Post—are, for the purposes of the *Privacy Act*, both an agency in respect of their non-commercial activities, and an organisation in respect of their commercial activities.[79]

18.68 As noted above, the OECD Guidelines apply to personal data in both the public and private sectors. Similarly, the principles in the APEC Privacy Framework and 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) also apply to both the public and private sectors.[80]

18.69 There is precedent in other jurisdictions for having a single set of principles applying both to the public and private sectors,[81] as well as for having separate principles or provisions regulating the public and private sectors.[82]

Previous privacy inquiries

18.70 The question whether to move to some form of unified privacy principles has been the subject of considerable debate in previous privacy inquiries.[83] In 2005, the OPC expressed its preference for a single set of principle principles:

> There seems no clear rationale for applying similar, but slightly different, privacy principles to public sector agencies and private sector organisations and certainly no clear rationale for applying both to an organisation at the same time. There is no clear policy reason why they are not consistent. The time may have come for a systematic examination of both the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations.[84]

18.71 Stakeholders making submissions to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry), and to the Taskforce on Reducing Regulatory Burdens on Business, expressed

---

78 See *Privacy Act 1988* (Cth) ss 95B, 6A(2).

79 Australia Post, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004. See *Privacy Act 1988* (Cth) s 7(c); *Freedom of Information Act 1982* (Cth) sch 2, div 1, pt II.

80 See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005); 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).

81 See, eg, *Privacy Act 1993* (NZ); *Data Protection Act 1998* (UK); *Personal Data (Privacy) Ordinance* (Hong Kong).

82 See, eg, *Privacy Act* RS 1985, c P-21 (Canada) (regulation of public sector); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) (regulation of private sector).

83 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005); Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006).

84 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 46.

concern about the inconsistency within the *Privacy Act* resulting from two sets of principles.[85] It was also noted that the existence of two separate regimes caused particular difficulties in the health sector, where public and private health organisations often work closely together.[86]

18.72 The Taskforce on Reducing Regulatory Burdens on Business recommended the development of a single set of privacy principles, applicable across the public and private sectors.[87] Similarly, the Senate Committee privacy inquiry ultimately recommended that the ALRC develop a single set of privacy principles.

> The committee recommends the development of a single set of privacy principles to replace both the National Privacy Principles and Information Privacy Principles, in order to achieve consistency of privacy regulation between the private and public sectors. These principles could be developed as part of the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2.[88]

Submissions and consultations

Responses to IP 31

18.73 The ALRC asked in IP 31 whether the IPPs and NPPs should be consolidated to create a single set of privacy principles applicable to both the public and private sectors and, if so, what model should be used. A related question was asked as to whether any particular principles, or exceptions to principles, should apply only to either the public or private sector.[89] It was noted in IP 31 that the number of similarities between the IPPs and NPPs appear to make the task of rationalisation feasible.[90]

18.74 In response to IP 31, a very large number of stakeholders submitted that it would be desirable to consolidate the IPPs and NPPs to create a single set of privacy principles, which would generally be applicable to organisations and agencies.[91]

---

85 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.35]; Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 56.

86 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.37].

87 See Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 56.

88 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 4, [7.9].

89 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–34.

90 Ibid, [4.193].

91 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Commission on Safety and Quality in Health Care, *Submission PR 252*, 14 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211*, 27 February 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; Law Council of Australia, *Submission PR 177*, 8 February 2007; Australian Privacy Foundation, *Submission PR 167*,

Stakeholders expressed support on the basis that maintaining separate sets of privacy principles creates complexity and confusion in a number of areas. It was submitted that a consolidation of the principles would simplify compliance requirements and, therefore, enhance administrative convenience.[92] In addition, stakeholders expressed the view that establishing a single set of privacy principles would help achieve the desirable goal of national consistency,[93] as well as consistency with a number of key international instruments, such as the EU Directive, the OECD Guidelines and the APEC Privacy Framework.[94]

18.75 A smaller number of stakeholders opposed moving to a single set of privacy principles.[95] Some stakeholders focused on the fact that sometimes it is necessary to impose different requirements on organisations and agencies.[96] Specifically, there was concern that the objects and functions of agencies differ from those of organisations and so it is appropriate to impose different privacy requirements on each.[97] For example, special principles may need to apply to the public sector because it can compel the production of personal information.[98] It was also suggested that it may be necessary to create a specific principle dealing with direct marketing that should apply only to the private sector.[99]

---

2 February 2007; Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007; Australian Health Insurance Association, *Submission PR 161*, 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; National E-health Transition Authority, *Submission PR 145*, 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 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; I Turnbull, *Submission PR 82*, 12 January 2007; Australia Post, *Submission PR 78*, 10 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007; National and State Libraries Australasia, *Submission PR 68*, 21 December 2006; The Mailing House, *Submission PR 64*, 1 December 2006.

92 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

93 Australian Commission on Safety and Quality in Health Care, *Submission PR 252*, 14 March 2007; Queensland Government, *Submission PR 242*, 15 March 2007; Fundraising Institute—Australia Ltd, *Submission PR 138*, 22 January 2007.

94 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

95 For example, Australian Direct Marketing Association, *Submission PR 298*, 29 June 2007; Confidential, *Submission PR 165*, 1 February 2007; AXA, *Submission PR 119*, 15 January 2007.

96 It should be noted, however, that some stakeholders argued that such inconsistencies as these could be accommodated by the *Privacy Act*: see Law Institute of Victoria, *Submission PR 200*, 21 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007.

97 Confidential, *Submission PR 165*, 1 February 2007.

98 Australian Direct Marketing Association, *Submission PR 298*, 29 June 2007; Confidential, *Submission PR 165*, 1 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007.

99 Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006. Direct marketing is dealt with in Ch 26.

Discussion Paper proposal

18.76 In DP 72, the ALRC proposed that the *Privacy Act* should be amended to consolidate the IPPs and NPPs into a single set of privacy principles—the UPPs—that would be generally applicable to agencies and organisations, subject to such exceptions as required.[100]

18.77 This proposal received overwhelming support,[101] with a number of stakeholders expressing strong support for such an approach.[102] Reasons for support included that unification would: enable easier compliance for organisations required to comply with both sets of principles;[103] result in administrative efficiencies;[104] and reduce complexity for organisations in areas where they contract to agencies and act as commercial operators.[105]

---

100 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007), Proposal 15–2.

101 BPay, *Submission PR 566*, 31 January 2008; Australian Government Department of Finance and Deregulation, *Submission PR 558*, 11 January 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; Google Australia, *Submission PR 539*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Medical Association, *Submission PR 524*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Australian Industry Group and Australian Electrical and Electronic Manufacturers' Association, *Submission PR 494*, 19 December 2007; National Children's and Youth Law Centre, *Submission PR 491*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007; Abacus–Australian Mutuals, *Submission PR 456*, 11 December 2007; Arts Law Centre of Australia, *Submission PR 450*, 7 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; Motor Traders Association of NSW, *Submission PR 429*, 10 December 2007; National Transport Commission, *Submission PR 416*, 7 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007; IBM Australia, *Submission PR 405*, 7 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; P Youngman, *Submission PR 394*, 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.

102 For example, Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

104 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007.

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

18.78 For example, IBM Australia submitted that it was very supportive of the proposal.

> As a large private organisation, IBM is required to comply with the NPPs. A major provider of IT products and services to the federal government, IBM is also required to comply with the IPPs as a 'contracted service provider' to the Commonwealth. Having only one privacy regime with which to comply will be much simpler for organisations such as IBM.[106]

18.79 PIAC submitted that:

> It makes no sense to continue the artificial dichotomy that exists in privacy regulation between the public and private sectors. This dichotomy is historically based, and appears to have no sound basis in policy …
>
> Having a single set of principles would reduce confusion and help to achieve national consistency as well as making Australian privacy regulation more consistent with international regimes.[107]

18.80 The National Transport Commission submitted that:

> Considering the increasing trend in regulatory reform towards utilising specialised external entities, particularly in the area of remote compliance monitoring (speed camera providers, external auditors etc) to provide services which the regulator is unable or unwilling to provide for various reasons (for example cost efficiencies) the consolidation of privacy principles would have positive benefits for regulators and those promulgating reforms which require the incorporation of privacy principles.[108]

18.81 Privacy NSW submitted that the proposed set of unified privacy principles represented

> a major step forward in harmonising Australian privacy laws and in eradicating the areas of overlap between the Commonwealth and the States … A common set of principles will allow for greater cooperation and pooling of resources among privacy agencies throughout Australia. It will also result in more cohesive decision-making across Australia and will make compliance by agencies and organisations more straightforward and therefore more comprehensive.[109]

18.82 Some stakeholders supported the proposal, but expressed reservations about either the drafting, implementation or administration of the UPPs. Namely:

- the Australian Federal Police expressed reservations about whether it would be possible to draft UPPs that address adequately the information collection, use, storage, destruction and disclosure needs of both the private and public sectors;[110]

---

106 IBM Australia, *Submission PR 405*, 7 December 2007.
107 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
108 National Transport Commission, *Submission PR 416*, 7 December 2007.
109 Privacy NSW, *Submission PR 468*, 14 December 2007.
110 Australian Federal Police, *Submission PR 545*, 24 December 2007.

- the Australian Institute of Company Directors emphasised that 'care needs to be taken [to ensure] that differences in structure and operations are taken into account';[111]

- Centrelink acknowledged the challenges of developing a single set of unified principles while maintaining a reasonable level of simplicity and clarity;[112]

- the Department of Agriculture, Fisheries and Forestry submitted that the development of one set of principles would present challenges in implementation;[113] and

- the Law Society of New South Wales submitted that the *Privacy Act* should also deal with the administration of the UPPs, stating that the public sector is generally better equipped than the private sector to administer privacy principles.[114]

18.83 Anglicare Tasmania expressed the view that, while the unification of the NPPs and IPPs would be of value, there is still a place for specific guidelines or codes for particular sectors.[115]

18.84 Only a very small number of stakeholders opposed the proposal. The Australian Direct Marketing Association (ADMA) submitted that it

> rejects expensive, unnecessary, radical and revolutionary wholesale reform, including the creation of Unified Privacy Principles (UPPs).
>
> In ADMA's view, the ALRC has not made the case that such a change would provide any great benefit to consumers or any great improvements to the private sector privacy regime which is, by and large, working well.[116]

18.85 A number of stakeholders expressed concern about naming the privacy principles the 'Unified Privacy Principles' on the basis that such a name would become irrelevant with the passage of time.[117]

---

111 Australian Institute of Company Directors, *Submission PR 424,* 7 December 2007.

112 Australian Government Centrelink, *Submission PR 555,* 21 December 2007

113 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556,* 7 January 2008.

114 Law Society of New South Wales, *Submission PR 443,* 10 December 2007.

115 Anglicare Tasmania, *Submission PR 514,* 21 December 2007.

116 Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007. ADMA's submission was supported by Axicom Australia: Acxiom Australia, *Submission PR 551,* 1 January 2008.

117 Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; K M Corke and Associates, *Submission PR 447,* 10 December 2007; Law Society of New South Wales, *Submission PR 443,* 10 December 2007. Some of these stakeholders submitted that such names as the 'Australian privacy principles' or 'Uniform privacy principles' were more appropriate.

ALRC's view

18.86 The overwhelming majority of stakeholders that expressed a view on this issue were in favour of consolidating the IPPs and NPPs to create a single set of privacy principles that generally would be applicable to organisations and agencies. In addition, there was support for the proposal from each of the various categories of stakeholder—that is, organisations, agencies and others. In the ALRC's view, the IPPs and NPPs should be consolidated to establish the UPPs that generally would be applicable to agencies and organisations.

18.87 A large number of benefits would flow from such a reform. For example, the move to a set of UPPs would foster national and international consistency in privacy regulation. Such a reform also would clarify and simplify the obligations of agencies and organisations with respect to information privacy. This would be advantageous for individuals who interact with these entities, and also for the agencies and organisations themselves, as they would not have to differentiate between the overlapping requirements of the IPPs and NPPs. Where an organisation is acting as a contracted service provider or is involved in a public-private partnership, it would reduce significantly the problems associated with the organisation having to comply with both the IPPs and NPPs. This simplification may go some way to offsetting costs associated with implementing a new regime for privacy regulation.[118]

18.88 The UPPs, however, should not apply rigidly to both agencies and organisations. As explained in the remaining chapters in this Part, some principles in the UPPs should apply only to organisations.[119]

18.89 As explained earlier in this chapter, the ALRC, for the purposes of this Report, refers to the single set of privacy principles as the model 'Unified Privacy Principles'. It is not, and never was, the ALRC's intention for that term to be adopted in the *Privacy Act*. If the ALRC's recommendation to adopt a single set of principles in the *Privacy Act* is adopted, it is likely to be appropriate to use a different term to describe the privacy principles. The ALRC agrees that the term model 'Unified Privacy Principles' will be otiose in the future. The decision of how best to describe the single set of privacy principles for the purposes of the *Privacy Act* will be a matter for the Office of Parliamentary Counsel.

---

118 The ALRC considers that the NPPs should form the general template in drafting and structuring the UPPs. This approach, which is discussed further below, should also help to minimise the transitional costs for organisations.

119 See Chs 26, 30.

Recommendation 18–2 The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles, referred to in this Report as the model Unified Privacy Principles.

Application of the Unified Privacy Principles

Background

18.90 What is the extent of the application of the UPPs? In particular, when can they be displaced by other obligations concerning the handling of personal information?

18.91 Under the ALRC's recommended regulatory model, regulations, consistent with the objects of the *Privacy Act*, can be introduced to provide greater specificity and certainty in regulating privacy in relation to particular activities. Those regulations would be more detailed and specific than the privacy principles and, where appropriate, they would be able to derogate from the requirements in the privacy principles by providing different (that is, more or less stringent) requirements than are provided for in the principles.[120]

Submission and consultations

18.92 In DP 72, the ALRC proposed that the model UPPs should apply to information privacy except to the extent that the *Privacy Act*, subordinate legislation under the *Privacy Act*, or another piece of Commonwealth legislation imposes different or more specific requirements in a particular context.[121]

18.93 This proposal received general support.[122] Some stakeholders, however, expressed concern that the proposal could allow less stringent requirements to be imposed and, therefore, legitimate a progressive 'watering down' of the UPPs through other Commonwealth legislation and subordinate legislation.[123] Views were expressed

120 See Chs 4, 5. See also Rec 5–1.

121 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007), Proposal 15–3.

122 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; Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Legal Aid Queensland, *Submission PR 489*, 19 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.

123 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

that any different or more specific requirements should offer an equivalent[124] or more stringent level of protection than the UPPs.[125]

18.94 The Cyberspace Law and Policy Centre supported the proposal but only

> to the extent that such differences or greater detail are justified. If it is possible for the UPPs to cover a situation, it is desirable that they do so. Even where differences of substance or detail are justified on some specific points, it is generally desirable for the UPPs to apply, and for a separate specific provision to provide the amending difference or detail. This will maximise the consistent application of interpretations by Courts and tribunals.[126]

18.95 National Archives of Australia noted that the disposal authority regime under the *Archives Act 1983* (Cth) could be undermined. It was concerned that the authorities under this regime would not qualify as pieces of Commonwealth legislation.[127]

18.96 BPAY opposed the proposal insofar as it dealt with other pieces of Commonwealth legislation.

> BPAY disagrees with this proposal to have numerous separate pieces of legislation. To the extent possible, the aim of this privacy review should be to construct the privacy regime in one piece of legislation. In recognition of the benefits of simplifying privacy, BPAY supports privacy legislation consolidated at federal level in the *Privacy Act*.[128]

ALRC's view

18.97 For the reasons discussed in Chapters 4 and 5, the model UPPs should apply to information privacy, except to the extent the *Privacy Act*, subordinate legislation under the *Privacy Act* or another piece of Commonwealth legislation imposes different or more specific requirements in a particular context.[129] This approach is necessary to allow for flexibility in specific situations.

18.98 By acknowledging that another piece of Commonwealth legislation may displace the operation of the UPPs, the ALRC is not intending to encourage the unbridled proliferation of Commonwealth statutes dealing with privacy. Rather, this approach recognises that it is legitimate for other pieces of Commonwealth legislation to deal with aspects of information privacy in specific contexts, including telecommunications. Discrete examples of such types of legislation include the

---

124 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

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

127 National Archives of Australia, *Submission PR 414*, 7 December 2007. Section 24(1) of the *Archives Act 1983* (Cth) provides, in part, that a person must not engage in conduct that results in the destruction, disposal or alteration of a Commonwealth record. However, s 24(2) provides that this does not apply to anything done with the permission of National Archives or in accordance with a practice or procedure approved by National Archives.

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

129 See Rec 5–1.

Telecommunications Act 1997 (Cth), the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).[130]

18.99 Further, regulations made under the *Privacy Act* that impose different or more specific requirements, of either greater or less stringency than those imposed by the UPPs, would nonetheless need to be consistent with the objects of the *Privacy Act*.[131]

Scope and structure of Unified Privacy Principles

Scope of Unified Privacy Principles

18.100 In considering the content of the privacy principles, the first question is: what should be the scope of the UPPs? In other words, should the scope of the UPPs match that of the IPPs, NPPs or both; or should the scope be narrower or broader?

18.101 Taken together, the IPPs and NPPs cover the following aspects of privacy in relation to personal information: collection; use and disclosure; data quality; data security; openness; access and correction; the adoption, use and disclosure of identifiers; the principle of anonymity; the regulation of transborder data flows; and the special protections that should apply to sensitive information.

18.102 At a minimum, the UPPs should cover the same aspects of privacy as are currently covered by the IPPs and NPPs, when taken together. This coverage is broadly consistent with the privacy regimes of other jurisdictions and at international law. The question whether the scope of the UPPs should be expanded to cover additional aspects of privacy is discussed in Chapter 32.

Structure of a single set of privacy principles

Background

18.103 Assuming the IPPs and the NPPs are consolidated to create a single set of privacy principles, a question arises as to how the UPPs should be structured. Specifically, should the UPPs be based on the NPPs, the IPPs or neither?

18.104 The privacy statutes of Victoria, Tasmania and the Northern Territory are largely based on the NPPs—although they are not 'word for word' replicas.[132] In each case, the NPPs have been used as a basis for the principles that are to apply to public sector bodies—although the Tasmanian provisions also apply to 'any body, organisation or person who has entered into a personal information contract relating to

130 See discussion in Part J of this Report.
131 See discussion in Ch 5.
132 See *Information Privacy Act 2000* (Vic) sch 1; *Personal Information Protection Act 2004* (Tas) sch 1; *Information Act 2002* (NT) sch 2.

personal information'.[133] In addition, the South Australian Department of Health and Department for Families and Communities have both adopted the NPPs, which 'demonstrat[es] the ability of the NPPs to be applied in a public sector setting'.[134] On the other hand, the privacy legislation of New South Wales and the privacy schemes in Queensland and South Australia resemble more closely the IPPs.[135]

18.105 One key consideration in determining the model of privacy principles to be applied is the compliance burden that will be imposed on agencies and organisations that have tailored their compliance systems to the requirements of the IPPs and the NPPs. Departing radically from those principles would increase the consequential compliance burden imposed on those entities that are to be subject to the UPPs. The OPC concluded that the NPPs 'have worked well and delivered to individuals protection of personal and sensitive information in Australia in those areas covered by the Act'.[136] The Senate Committee privacy inquiry, however, disagreed with the OPC's conclusion that the private sector provisions are 'working well'.[137]

Submissions and consultations

18.106 Before the release of DP 72, a number of stakeholders expressed the view that the NPPs—though capable of improvement—are superior to the IPPs and should form the model for any set of UPPs.[138]A small number of stakeholders stated that, if there were to be one set of privacy principles, it would be preferable to develop a new set of principles rather than merely merging and modifying the existing NPPs and IPPs.[139]

18.107 In DP 72, the ALRC proposed that the NPPs should provide the general template in drafting and structuring the proposed UPPs.[140] This proposal was widely supported.[141] Reasons for support included that:

---

133 See *Personal Information Protection Act 2004* (Tas) s 3.

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

135 See *Privacy and Personal Information Protection Act 1998* (NSW) pt 2, div 1; Queensland Government Department of Justice and Attorney-General, *Privacy* <www.justice.qld.gov.au/40.htm> at 5 May 2008; South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

136 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 2–3.

137 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.27].

138 See, eg, Government of South Australia, *Submission PR 187*, 12 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; AAMI, *Submission PR 147*, 29 January 2007; D Antulov, *Submission PR 14*, 28 May 2006.

139 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006.

140 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007), Proposal 15–4.

141 Government of South Australia, *Submission PR 565*, 29 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 2007; Australian Taxation Office, *Submission PR 515*, 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; Legal Aid Queensland, *Submission*

- the NPPs were developed in consultation with stakeholders;[142]

- departure from the NPPs in the UPPs is likely to increase compliance costs for organisations that have already invested significant resources in ensuring compliance with the NPPs;[143]

- the NPPs are simpler, more concise, and more user-friendly than the IPPs;[144] and

- the ability of the NPPs to translate well into the public sector has already been demonstrated by the privacy statutes of Victoria, Tasmania and the Northern Territory.[145]

18.108 A small number of stakeholders expressed concerns that a move to UPPs based on the NPPs would impose a considerable transitional burden and cost for the public sector.[146] Some agencies also expressed the view that the wording of the IPPs is clearer and more concise than that of the NPPs.[147]

18.109 Other stakeholders put forward alternative models for drafting the UPPs. The Office of the Victorian Privacy Commissioner submitted that:

> Any template used to draft the UPPs should be set at the highest standard of privacy protection. While the NPPs generally set a high standard of privacy protection, they do not provide the same level of protection as the Victorian IPPs, particularly where the privacy principle concerning 'sensitive information' and 'unique identifiers' are concerned.[148]

PR 489, 19 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; Australian Finance Conference, *Submission PR 398*, 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.

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

143 BPay, *Submission PR 566*, 31 January 2008; Optus, *Submission PR 532*, 21 December 2007; Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007. The Centre for Law and Genetics expressed a similar view that adopting the NPPs would minimise compliance burden and costs: Centre for Law and Genetics, *Submission PR 497*, 20 December 2007.

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

145 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. One stakeholder expressed the view that the UPPs should be identical to the NPPs unless there were compelling reasons not to adopt that approach: BPay, *Submission PR 566*, 31 January 2008.

146 Medicare Australia, *Submission PR 534*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

147 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

148 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

18.110 The Australian Federal Police supported the proposal in principle but expressed the view that

> the more recent privacy legislation enacted in NSW, Victoria and Queensland should be considered as well—for example, their approach to dealing with law enforcement requirements.[149]

ALRC's view

18.111 The general structure of the NPPs has been largely effective. This is borne out by the response of stakeholders to this Inquiry, the majority of which have indicated that they are generally satisfied with the structure of the NPPs. It is also noted that adopting a radically different structure from the NPPs would involve a greater compliance burden, particularly on organisations that have to update their privacy protection regimes.

18.112 Consequently, the NPPs should form the general template in drafting and structuring the UPPs. Having drafted model UPPs, and made other recommendations concerning their content, there is no need to make a specific recommendation in this regard.

18.113 In adopting this approach, two important points should be made. First, the ALRC's general view that the NPPs should form the template for the UPPs is not intended to impact on the *substantive content* of the UPPs; rather it is intended only to guide the *general form* or framework of the UPPs. Secondly, the ALRC does not consider it appropriate for the statutory drafters to follow strictly the NPPs structure or wording where it is obvious that amendments can be made that would improve on the status quo. It would be entirely appropriate for the UPPs to depart from the general structure of the NPPs in such circumstances. This general approach is reflected in the way in which the model UPPs have been drafted by the ALRC in this Report.

149 Australian Federal Police, *Submission PR 545*, 24 December 2007.

19. Consent

Contents

Introduction

19.1 Consent is not a privacy principle in itself. It is relevant, however, to the operation of some privacy principles, namely those dealing with the collection of sensitive information, use and disclosure, and cross-border data flows. In certain instances, the provision of consent can provide legal authority for an agency or organisation to deal with an individual's personal information in a particular way.

19.2 This chapter considers consent as it applies to the privacy principles in the *Privacy Act 1988* (Cth), and other issues concerning consent, in particular the use of bundled consent. It considers whether the definition of 'consent' in the *Privacy Act* should be amended or be the subject of more detailed guidance from the Office of the Privacy Commissioner (OPC). Finally, the chapter canvasses whether the model Unified Privacy Principles (UPPs) should contain a separate principle dealing with consent.

Background

Role of consent in the privacy principles

19.3 As stated above, consent is only relevant to the application of a some privacy principles. Consent is either framed as an exception to a general prohibition against personal information being handled in a particular way or as a basis to authorise the handling of personal information in a particular way. Significantly, in each case,

consent is not the only exception to a stated prohibition, nor the only basis for permitting the handling of personal information in a particular way.

19.4 The Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) do not require that an individual give his or her consent to the collection of that individual's personal information. There is, however, a general prohibition against an organisation collecting sensitive information about an individual. One of the exceptions to that prohibition is where the individual has given consent.[1]

19.5 There is a general prohibition against an organisation using or disclosing personal information about an individual for a purpose other than the primary purpose of collection. One of the exceptions to that prohibition is where an individual has given consent to the use or disclosure.[2]

19.6 Similarly, there is a general prohibition against an agency using information obtained for a particular purpose for any other purpose.[3] One of the exceptions to that prohibition is where the individual concerned has consented to the use of the information for that other purpose.[4] Further, the general prohibition against an agency's ability to disclose personal information does not apply where the individual has consented to the disclosure.[5]

19.7 An organisation is only authorised to transfer an individual's personal information to a foreign country in defined circumstances.[6] One of those circumstances is where the individual consents to the transfer.[7]

Meaning and elements of consent

19.8 The term 'consent' is defined in the *Privacy Act* to mean 'express consent or implied consent',[8] but remains otherwise undefined. The Macquarie Dictionary defines 'consent' as being 'to give assent; agree; comply or yield'.[9]

---

1 *Privacy Act 1988* (Cth) sch 3, NPP 10.1(a).
2 Ibid sch 3, NPP 2.1(b).
3 Ibid s 14, IPP 10.1.
4 Ibid s 14, IPP 10.1(a).
5 Ibid s 14, IPP 11.1(a).
6 Ibid sch 3, NPP 9.
7 Ibid sch 3, NPP 9(b). Under the ALRC's recommended principle dealing with 'Cross-border Data Flows', consent to transfer is one of a number of bases upon which an agency or organisation can transfer personal information overseas without remaining accountable for that personal information. See Ch 31.
8 Ibid s 6(1).
9 *Macquarie Dictionary* (online ed, 2007).

19.9 The concept of consent arises in many different contexts. The *Privacy Act* does not affect the general law applicable to consent. The requisite elements of consent must be met, therefore, including voluntariness; and capacity to understand, provide and communicate.[10]

19.10 Whether consent is voluntary depends on whether an individual has a clear option not to consent. Relevant to this assessment is whether receiving the option not to consent, and withholding consent itself, involves no financial cost to, and little effort from, the individual.[11] A further relevant consideration is whether an individual's option to consent to one purpose is freely available and not bundled with other purposes.[12]

19.11 The need for consent to be voluntary and informed in information privacy contexts has been emphasised in a number of existing guidelines,[13] international instruments,[14] regional models,[15] and overseas legislation.[16] The OPC has generally explained the concept of consent as follows:

> Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. Consent is invalid if there is extreme pressure or coercion.
>
> Only a competent individual can give consent although an organisation can ordinarily assume capacity unless there is something to alert it otherwise. Competence means that individuals are capable of understanding issues based on reasoned judgements

---

10 J Douglas-Stewart, *Annotated National Privacy Principles* (3rd ed, 2007).

11 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341, 364–365.

12 In Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.46], it was stated that the practice of bundling consents has the potential to undermine the voluntariness of consent of an applicant for insurance. Bundled consent is discussed further below.

13 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001); Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001); National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007). In Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.27]; [28.34]–[28.37], the ALRC also emphasised the importance of consent being informed and voluntary.

14 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).

15 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.

16 For example, *Personal Data Act 1998* (Sweden) s 3, which defines consent as 'every kind of voluntary, specific and unambiguous expression of will by which the registered person, after having received information, accepts processing of personal data concerning him or her'.

> and communicating their decisions. The general law about competence and incapacity will apply to the issue of consent.[17]

19.12 The OPC's *Guidelines on Privacy in the Private Health Sector*[18] (the Health Guidelines) explain the key elements of consent as follows:

> Consent must be voluntary—the individual must have a genuine opportunity to provide or withhold consent; that is, they must be able to say 'yes' or 'no' without extreme pressure which would equate to an overpowering of will.
>
> Consent must be informed—the individual must know what it is they are agreeing to. In other words, the individual needs to be aware of the implications of providing or withholding consent, having received the information in a way meaningful to them and appropriate in the circumstances.
>
> The individual must have the capacity to provide consent—the individual must be capable of understanding the issues relating to the decision, forming a view based on reasoned judgment and communicating their decision.[19]

19.13 The National Statement on Ethical Conduct in Human Research (National Statement) provides guidance concerning consent to participate in research, and states, in part, that:

> The requirement [for consent] has the following conditions: consent should be a voluntary choice, and should be based on sufficient understanding and adequate understanding of both the proposed research and the implications of participation in it …
>
> The process of communicating information to participants and seeking their consent should not be merely a matter of satisfying a formal requirement. The aim is mutual understanding between researchers and participants …
>
> No person should be subject to coercion or pressure in deciding whether to participate.[20]

19.14 The European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* (EU Directive), defines 'the data subject's consent' as 'any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him to be processed'.[21]

19.15 The draft Asia-Pacific Privacy Charter provides that consent should be 'freely-given, informed, variable and revocable'. It states that consent is 'meaningless if

---

17 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 22.
18 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001).
19 Ibid, [A.5.2].
20 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), Ch 2.2.
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), art 2(h).

people are not given full information, or have no option but to consent in order to obtain a benefit or service'.[22]

19.16 What is required to demonstrate that consent has been obtained from an individual remains a live issue in privacy regulation. Specific requirements are often highly dependent on the context in which the personal information is collected, used or disclosed, including how the consent is sought, and the characteristics of the individual from whom consent is sought. For example, the National Statement:

> Consent may be expressed orally, in writing or by some other means (for example, return of a survey or conduct implying consent) depending on:
>
> (a) the nature, complexity and level of risk of the research; and
>
> (b) the participant's personal and cultural circumstances.[23]

19.17 In the context of giving guidance in relation to the use and disclosure of personal information for a purpose other than the primary purpose of collection, the OPC has stated:

> It may be possible to infer consent from the individual's failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up. If the organisation's use or disclosure has serious consequences for the individual, the organisation would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In such situations it would ordinarily be more appropriate for the organisation to seek express consent.[24]

19.18 The OPC has issued a number of 'tips for compliance' in relation to establishing consent, including:

> An organisation would have the most difficulty establishing consent to a use or disclosure where it wishes to rely on a failure to object to a use or disclosure to imply consent …
>
> An organisation will be in an increasingly better position to establish that the individual consented the more it can satisfy the following points:
>
> - it is likely that the individual received and read the information about the use or disclosure;

---

22 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 2.

23 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), Ch 2.2.

24 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 37. This guidance replicates what was stated in the Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [344]. Some privacy advocates have criticised the OPC's guidance in this regard: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

- the chance to opt out of the offer is clearly stated and likely to be understood by the individual and the individual is likely to be aware of the implications of not opting out;
- the opting in or opting out is freely available and not bundled with other purposes;
- receiving the chance to opt out involves no financial cost to, and little effort from, the individual;
- opting out involves little effort from, and no or virtually no cost to the individual;
- the consequences of failing to opt out are harmless;
- if the individual opts out later, the individual is fully restored, where possible and appropriate, to the circumstances they would have been in if they had opted out earlier.[25]

19.19 The Health Guidelines note that there are situations where health service providers reasonably may rely on implied consent from individuals to handle health information in particular ways. The following example is given:

> If a medical practitioner collects a specimen to send to a pathology laboratory for testing, it would be reasonable to consider that the individual is giving implied consent to the passing of necessary information to that laboratory.[26]

19.20 The Health Guidelines provide also that where consent is required to collect and use personal information for public health purposes, such as those concerning the establishment and maintenance of a disease register, it may sometimes be appropriate to give individuals the opportunity to opt out of being included on the register. They provide that such an approach only would be appropriate 'where individuals are clearly informed about the option to opt out and it is prominently presented and easy to adopt'.[27]

19.21 In exploring the general meaning of consent in privacy law, it is useful also to refer to other jurisdictions. Most comparable foreign jurisdictions do not provide a detailed statutory definition of consent in their privacy legislation. For example, consent is not defined in the *Data Protection Act 1998* (UK).

19.22 There are, however, some examples of comparatively detailed statutory provisions regulating consent. Italian information privacy law contains a provision called 'consent' that states:

---

25 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 38.
26 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), [A.5.3].
27 Ibid, [A.5.3].

> 1. Processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent.
> 2. The data subject's consent may refer either to the process as a whole or to one or more of the operations thereof.
> 3. The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13.
> 4. Consent shall be given in writing of the processing concerns sensitive data.[28]

19.23 German privacy legislation requires that consent be based on a 'free decision of the data subject'; that it be in writing except where special circumstances render some other form appropriate; and that the consent refer expressly to the collection, process or use of 'special categories of personal data'.[29]

19.24 The *Model Code for the Protection of Personal Information*, which is set out in Canada's *Personal Information Protection and Electronic Documents Act 2000* (PIPED Act), states that, in obtaining consent, the reasonable expectations of the individual are relevant. The Model Code also states that organisations generally should seek express consent when the information is likely to be considered sensitive, and that implied consent generally would be appropriate when the information is less sensitive.[30]

Bundled consent

19.25 Bundled consent refers to the practice of an agency or organisation 'bundling' together, or consolidating, multiple requests for an individual's consent to a wide range of uses and disclosures of personal information, without giving the individual the option of selecting to which uses and disclosures he or she agrees. Bundled consent is often sought as part of the terms and conditions of a product or service.[31]

19.26 Submissions from consumer groups to the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) were highly critical of the practice, stating, for example, that it undermines the requirement that consent be meaningful, informed and freely given.[32] Similar sentiments were expressed to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry). For example, one stakeholder stated that it was difficult

---

28 *Personal Data Protection Code 2003* (Italy) s 23.
29 *Federal Data Protection Act 1990* (Germany) s 4(a).
30 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principle 4.35, 4.36.
31 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 82.
32 Ibid, 85.

for individuals to give free and informed consent when presented only with broad or vague statements concerning possible use and disclosure, or when told that services would not be provided in the absence of consent.[33]

19.27 On the other hand, there may be circumstances in which organisations legitimately seek bundled consent from consumers. The business sector, and particularly the finance and telecommunications industries, emphasised to the OPC Review and the Senate Committee privacy inquiry the need to seek bundled consent in order to achieve business efficiency and reduce costs to the consumer. For example, telecommunications organisations submitted that to obtain consent for each specific use of an individual's personal information would significantly increase the complexity and costs of compliance. These costs, they argued, would inevitably be passed on to the consumer.[34]

19.28 The finance industry emphasised that seeking a single consent for multiple uses of information—for example, in an application for finance—was necessary to ensure that the information could be used not only to process the application, but to manage the account, administer insurance claims, recover money owed and maintain the value of the asset.[35] In 2005, the OPC stated that it would develop guidelines on bundled consent.[36]

Submissions and consultations

Meaning of consent

19.29 In Discussion Paper 72, *Review of Australian Privacy Law* (DP 72), the ALRC canvassed a number of options for reform to clarify the meaning of consent as it applies to the privacy principles. These options included:

- amending the *Privacy Act* to set out:
    - in detail what is required to obtain the requisite consent in the many contexts in which it may be sought under the Act, and with greater precision, the factors that should be taken into account in obtaining an individual's consent;

---

33 See Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.140]–[4.141].

34 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 86. See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.142]–[4.143].

35 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 86.

36 Ibid, rec 22.

- requiring the OPC to provide more guidance on what constitutes consent for the purposes of the privacy principles in various contexts; or

- combining elements of the above approaches.[37]

19.30 The ALRC formed the preliminary view that consent should be dealt with through further OPC guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. The ALRC proposed that this guidance should cover consent as it applies in various contexts, and should include advice on when it is and is not appropriate to use the mechanism of bundled consent.[38]

19.31 Most stakeholders supported the ALRC's proposal.[39] A number of stakeholders expressed the view that the provision of guidance was preferable to amending the statutory definition of consent.[40] For example, the Federation of Community Legal Centres (FCLC) submitted that:

> Due to the complexity of the issues, the proposal that the OPC provide further guidance to agencies and organisations about what is required to obtain an individual's consent is probably the most realistic of the … options suggested.[41]

---

37 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007), [16.26]–[16.35].

38 Ibid, Proposal 16–1. Stakeholders' views on the ALRC's approach to bundled consent are addressed separately below.

39 Government of South Australia, *Submission PR 565,* 29 January 2008; Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007; Australian Government Department of Human Services, *Submission PR 541,* 21 December 2007; Medicare Australia, *Submission PR 534,* 21 December 2007; Optus, *Submission PR 532,* 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525,* 21 December 2007; Anglicare Tasmania, *Submission PR 514,* 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; New South Wales Aboriginal Justice Advisory Council, *Submission PR 501,* 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; Legal Aid Queensland, *Submission PR 489,* 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; Australian Government Department of Defence, *Submission PR 440,* 10 December 2007; Australasian Compliance Institute, *Submission PR 419,* 7 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; Mortgage and Finance Association of Australia, *Submission PR 344,* 19 November 2007.

40 See, eg, Optus, *Submission PR 532,* 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525,* 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.

41 Federation of Community Legal Centres (Vic), *Submission PR 509,* 21 December 2007.

19.32 The OPC submitted that it would not support approaches to amend the current definition of consent or to set out consent requirements for a given sector in legislative provisions.

> These options risk introducing greater complexity into privacy regulation without having demonstrated a deficiency in the current consent framework. Accordingly, the [OPC] suggests that guidance material is the best approach to reducing uncertainty on consent requirements.[42]

19.33 Stakeholders emphasised the value of guidelines in clarifying legislation, enhancing compliance, promoting consistent implementation, increasing public awareness, and maintaining flexibility.[43] The FCLC, however, pointed out that

> a significant weakness of the 'guidance' approach is that by definition, it does not require organisations and agencies to behave in the manner suggested, and cannot specify that there will be legal consequences if they do not adequately consider whether consent has genuinely been obtained. Instead, it is left to the courts to develop the law. This approach therefore risks simply retaining the burden of upholding privacy rights on aggrieved parties, often those least likely to make a complaint.[44]

19.34 Stakeholders emphasised the importance of the guidance being developed in consultation with relevant bodies, including state and territory privacy commissioners,[45] marginalised communities and their advocates,[46] various industry sectors,[47] agencies and organisations.[48] For example, the OPC suggested that it consult with agencies, organisations and other stakeholders to determine the need for, and content of, guidance material relating to consent in various contexts.[49]

19.35 Stakeholders expressed views about the content of the OPC's guidance. There was support for the guidance to address the:

---

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

43 Australian Government Department of Broadband, Communications and the Digital Economy, *Submission PR 512*, 21 December 2007; Australasian Compliance Institute, *Submission PR 419*, 7 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.

44 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007.

45 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

46 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007.

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

48 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. The National Health and Medical Research Council stated that it would be pleased to assist in the development of guidance on consent in the context of health care and research: National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

- age at which consent can be given;[50]

- issues relating to consent for vulnerable populations in a service delivery context, especially as it applies to dealings in sensitive information;[51] and

- essential elements of consent: namely that consent be voluntary, informed, specific and current, and that the individual concerned has capacity to consent.[52]

19.36 The National Health and Medical Research Council, however, submitted that it was imperative that the capacity to obtain extended and unspecified consents for research purposes, as described in the *National Statement on Ethical Conduct in Human Research*,[53] is retained.[54]

19.37 The FCLC noted the elements of consent identified by the ALRC in DP 72, namely, the context in which consent is sought; and whether the consent is informed, voluntary and freely available. It submitted that:

> These factors are often intertwined and are all underpinned by social disadvantage …
>
> We would add to these considerations a further emphasis that the factors to be assessed may not be simply personal to individuals; rather they also arise from people's membership of communities which are structurally disadvantaged. For example, a young Sudanese man whose experience of officialdom is limited to over-policing is unlikely to have confidence that if he is requested to provide data he can legitimately refuse. However, his response may be wrongly interpreted as simple personal passivity.[55]

19.38 Microsoft Asia Pacific submitted that the OPC's guidance on consent should include a 'tiered consent model'. It stated:

> A tiered consent model seeks to tie the minimum permissible level of consent that a regulated entity must obtain to the risk inherent in the proposed activity involving an individual's personal information. For example, the privacy risk associated with the collection, use or disclosure of sensitive information is quite high, so regulated entities should be required to obtain explicit, opt-in consent from individuals.

---

50 Pharmacy Guild of Australia, *Submission PR 433*, 10 December 2007. One stakeholder submitted that there were particular situations where children and young people should be able to seek medical assistance without parental consent: New South Wales Aboriginal Justice Advisory Council, *Submission PR 501*, 20 December 2007.

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

52 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. The Queensland Government supported, in general terms, provision by the OPC of guidance on the nature of, and requirements for, valid consent in particular circumstances: Queensland Government, *Submission PR 490*, 19 December 2007.

53 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

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

55 Federation of Community Legal Centres (Vic), *Submission PR 509*, 21 December 2007.

> Where the privacy risk is lower, for example, where an organisation proposes to use or disclose non-sensitive personal information for a secondary purpose, regulated entities should be able to obtain consent by offering individuals a meaningful opportunity to opt-out of the proposed use or disclosure. Finally, where the privacy risk is lowest, it should be sufficient for a regulated entity to obtain implied consent from the data subject based on the organisation's notification of the proposed dealing and the data subject's subsequent conduct.[56]

19.39 A smaller number of stakeholders, however, submitted that proposing further OPC guidance on consent was not enough, and that the *Privacy Act* should be amended to include a more detailed definition of consent.[57] Some stakeholders submitted that the definition should set out a non-exhaustive list of factors to be taken into account in determining whether a person's consent has been obtained.[58]

19.40 The Public Interest Advocacy Centre (PIAC) submitted that:

> Unless the issue of consent is clearly understood and consistently applied, the privacy principles stand on fragile foundations. There clearly needs to be greater clarity as to the meaning of consent in the *Privacy Act*. Rather than hiving off this problem to the OPC to deal with in yet more guidelines, the ALRC should recommend that the definition of 'consent' in the *Privacy Act* should be amended to set out with greater precision what factors need to be taken into account in obtaining a person's consent or determining whether or not consent has been given …
>
> PIAC agrees that consent will inevitably depend on context and that what is required to obtain consent in one situation may be different to what is required in another situation. However, it is possible to distil some core elements of consent, and these should be enshrined in legislation.[59]

19.41 Both Cyberspace Law and Policy Centre and the Australian Privacy Foundation submitted that the definition of consent should be amended to deal with a number of key issues concerning consent, including to prevent the abuse of bundled consent. They each expressed the view that the *Privacy Act*, or the explanatory memorandum, should provide that:

- implied consent must be clear and unambiguous;

---

56 Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007. The OPC agreed that 'the greater the sensitivity of the information or the practice, the more likely it is that consent should be expressed actively, rather than implied': Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

57 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; GE Money Australia, *Submission PR 537*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

58 See, eg, Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007.

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

- a mere failure to opt out cannot be regarded as consent, even where the opt out is clearly and prominently displayed; contrary to the OPC's guidance on this issue; and

- where a person has no choice but to provide information in order to obtain a benefit, no consent to any uses of that information beyond the express purpose of collection may be implied.[60]

Bundled consent

19.42 In response to IP 31, a large number of stakeholders expressed concern about the use of bundled consent. They noted that this requires individuals to adopt an all or nothing approach—that is, they are unable to specify what particular uses or disclosures are, and are not, acceptable to them.[61] One example given was of a real estate agent said to use a single form to request a prospective tenant's consent to the disclosure of personal information to the media, the landlord, residential tenancy databases and the local real estate industry body, even though each of these entities would use the information differently, and for different purposes.[62]

19.43 Stakeholders expressed particular concerns about circumstances in which a failure to provide consent leads to an agency or organisation withholding access to goods or services.[63] Some stakeholders observed, however, that sometimes an agency or organisation needs to use or disclose an individual's personal information to enable it to provide a particular service, and that in such circumstances it should be permitted to withhold the service unless consent is provided.[64]

19.44 The OPC submitted that

> where an agency or organisation wants to use information for a purpose other than [the purpose] for which it was collected, then the individual's consent should be sought for the extended use of that information but it should not be made a condition of the original service.[65]

---

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

61 See, eg, Australian Privacy Foundation, *Submission PR 167*, 2 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; Anglicare Tasmania, *Submission PR 135*, 19 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107*, 15 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007.

62 Anglicare Tasmania, *Submission PR 135*, 19 January 2007.

63 See, eg, AAMI, *Submission PR 147*, 29 January 2007; Confidential, *Submission PR 143*, 24 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.

64 Law Council of Australia, *Submission PR 177*, 8 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.

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

19.45 Some stakeholders submitted that bundling consent is necessary for practical reasons. These include:

- where an agency or organisation has multiple interactions with an individual client, and must therefore handle the individual's personal information many times;[66]

- where an organisation has a large number of clients, it can be 'impractical and unworkable' to allow customers to negotiate terms on an individual basis;[67] and

- sometimes there is a practical necessity to outsource parts of a business, which leads to a greater number of entities handling an individual's personal information.[68]

19.46 Some stakeholders submitted that this area of the law needs to be clarified,[69] and a number expressed support for OPC guidance on how and when to seek bundled consent.[70]

Discussion Paper proposal

19.47 As noted above, in DP 72, the ALRC proposed that the OPC provide further guidance on consent, including when it is and is not appropriate to use the mechanism of 'bundled consent'.[71] The ALRC's approach acknowledged that there may be circumstances where the use of bundled consent may be legitimate, and others where it will not.

---

66 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Telstra, *Submission PR 185*, 9 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100*, 15 January 2007.

67 AAPT Ltd, *Submission PR 338*, 7 November 2007.

68 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

69 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007.

70 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Telstra, *Submission PR 185*, 9 February 2007; Anglicare Tasmania, *Submission PR 135*, 19 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

71 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 16–1.

19.48 This approach received general support.[72] Some stakeholders welcomed the opportunity to participate in developing guidance in consultation with the OPC in relation to the use of bundled consent in their particular industries.[73] Others submitted that the OPC should engage with various industry sectors and other stakeholders, including state and territory privacy commissioners, in formulating such guidance.[74] The OPC noted that it is currently producing guidance material on bundled consent pursuant to the recommendation made in the OPC Review.[75]

19.49 Some stakeholders emphasised the benefits of bundled consent, including in terms of efficiency and practicality, especially for small business.[76] They submitted that prohibiting bundled consent would give rise to significant system issues and compliance costs. Contacting customers to seek separate consents would be expensive and result in costly information technology systems changes.[77]

19.50 Many stakeholders supported the proposed guidance validating the use of bundled consent in appropriate situations. For example, the Department of Defence submitted that the OPC's guidance should allow bundled consent to enable identity-related services to be provided to Defence personnel. It submitted that bundled consent

> is also required to enable appropriate audit, management, control and protection measures to be adopted for identity related information, especially when IT-management 'best practice' regularly changes with the emergence of new technology to perform basic data management functions, such as backup and restore.[78]

---

72 See, eg, Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Anglicare Tasmania, *Submission PR 514*, 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; Legal Aid Queensland, *Submission PR 489*, 19 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; Australia Post, *Submission PR 445*, 10 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

73 See, eg, Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Australian Collectors Association, *Submission PR 505*, 20 December 2007.

74 Confidential, *Submission PR 536*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

75 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 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 22.

76 See, eg, Confidential, *Submission PR 519*, 21 December 2007; ANZ, *Submission PR 467*, 13 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007; Retail Motor Industry, *Submission PR 407*, 7 December 2007.

77 See, eg, Confidential, *Submission PR 536*, 21 December 2007; Confidential, *Submission PR 519*, 21 December 2007; BUPA Australia Health, *Submission PR 455*, 7 December 2007.

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

19.51 Stakeholders from the financial services industry supported the use of bundled consent in that industry on the basis that it was legitimate, in accordance with feedback from customers that they do not want to be contacted for their consent for each component of a service, and necessary in order to reduce costs to the consumer and achieve business efficiency.[79] The Financial Planning Association submitted that:

> Typically in financial advice and product supply there exists a chain of relationships that would require complex and onerous consent arrangements if bundled consent is not permitted. This would not be in the interests of the end client and we suggest that appropriate guidance be provided to enable this type of scenario to be maintained.[80]

19.52 GE Money submitted that:

> A financial service provider taking information in an application from an individual may need to use that information to assess the application for credit, open an account, provide credit funds to the individual, maintain the account, and transact the account in accordance with the instructions of the customer on an ongoing basis …
>
> In many instances there will be no way in which the service provider can 'unbundle' the consent and still provide the product. Organisations may very genuinely not be able to exclude a particular use of information and still provide the product.[81]

19.53 Stakeholders from the telecommunications industry also supported the use of bundled consent.[82] AAPT opposed any change that would imply that bundled consent in contracts or Standard Form Agreements in the telecommunications industry may not be appropriate.

> The concept of Standard Form of Agreements is well known in industries where there are mass customers, and the ability for mass or residential customers to individually negotiate on these terms, particularly in relation to specific section of the Standard Form of Agreement is simply impractical and unworkable.[83]

19.54 Other stakeholders noted when bundled consent would be inappropriate. For example, Anglicare Tasmania, in supporting the proposal for guidance, submitted that:

> Real estate agents should not use bundled consent for any matter not directly related to processing the application [for lease](which would include confirming the applicant's identity and conducting reasonable reference checks) and managing any resulting tenancy (which would include provision of the tenant's contact details to trades people conducting essential repairs and maintenance and contacting the tenant about inspection times and dates or changes to the lease).[84]

---

79 See, eg, Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Financial Planning Association of Australia, *Submission PR 496*, 19 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007. Specific support was expressed for the use of bundled consent in the debt collection sector: Australian Collectors Association, *Submission PR 505*, 20 December 2007.

80 Financial Planning Association of Australia, *Submission PR 496*, 19 December 2007.

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

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

83 AAPT Ltd, *Submission PR 338*, 7 November 2007

84 Anglicare Tasmania, *Submission PR 514*, 21 December 2007.

19.55 A minority of stakeholders were of the view that the ALRC's proposal concerning guidance was insufficient. Some opposed the practice of bundled consent in any circumstances. Liberty Victoria submitted that:

> Under no circumstances is bundled consent adequate. Private information belongs to the individual. Use of their information requires that consent be informed, be voluntary, be freely available and not bundled with other purposes. Bundling not only undermines the voluntariness of consent but the right to privacy generally.[85]

19.56 Privacy advocates submitted that the definition of consent needs to be amended to prevent abuse of the practice of bundled consent and that, in particular, 'wherever consent is applicable to the operation of a privacy principle, separate consent should be required for each proposed purpose of use'.[86] PIAC submitted that bundled consent should be prohibited or subject to strict limitations.[87]

19.57 The Australian Digital Alliance expressed reservations about the likelihood of OPC guidance stopping organisations from using bundled consent in inappropriate circumstances. It noted that:

> Consumers are very often subject to 'bundled consents' in relation to Digital Rights Management (DRM). Products containing DRM technology often require a consumer to click 'I agree' to all the terms and conditions, which include privacy provisions. These provisions can involve giving consent to collection of a broad range of personal information, and use of the consumer's information in a wide range of ways, including permission to pass information on to third parties. In many cases there is little justification (other than profiling or marketing) for the organisation to be collecting this personal information.[88]

ALRC's view

Meaning of 'consent'

19.58 The most appropriate way to clarify the meaning of consent, as it applies to the privacy principles, is for the OPC to provide further guidance in this regard. The guidance should address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained.

19.59 There is a pressing need for contextual guidance on consent. What is required to demonstrate that consent has been obtained is often highly dependant on the context in which personal information is collected, used and disclosed. The ALRC, therefore, recommends that the OPC's guidance should cover express and implied consent as it applies in various contexts, such as those that arise in transactions concerning financial

---

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

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

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

88 Australian Digital Alliance, *Submission PR 422,* 7 December 2007.

services, credit reporting, telecommunications, health services and research, and service delivery. The guidance could address, for example, circumstances in which reliance on express consent is preferable to reliance on implied consent.

19.60 While some factors that are relevant in assessing whether consent has been obtained will likely remain constant in all contexts—for example, the requirements that consent be voluntary, informed and given by an individual with capacity to understand—there may need to be flexibility in the treatment of other factors. For example, in some contexts it will be appropriate for consent to be obtained in relation to a *specific* collection, use, disclosure or cross-border transfer; whereas for research purposes, it may be legitimate for an informed individual to be able to give extended and unspecified consent, as described in the National Statement.[89]

19.61 Amending the *Privacy Act* to set out in detail what is required to obtain the requisite consent in the many contexts in which it may be sought is problematic. This approach would require a very large number of prescriptive rules that attempt to cover the wide variety of situations in which an agency or organisation may seek consent to deal with an individual's personal information. Such an approach would be inconsistent with the ALRC's view that a principles-based approach should continue to be at the heart of the *Privacy Act*.[90] Moreover, such an approach would be doomed to fail because it would be very difficult, if not impossible, to cover every relevant context.

19.62 The merits of amending the definition of consent in the *Privacy Act* to include, for example, the elements of consent, are also questionable. The concept of consent is not peculiar to privacy law. The common law has an important role to play in determining the elements of consent. A statutory definition is unable to capture nuances in the evolution of the common law and may have unintended consequences. The definition may be interpreted too restrictively, creating an undesirable restriction on the flow of information. Significantly, it tends to be civil law jurisdictions that possess a detailed statutory definition of consent. In these jurisdictions, such a process of codification may be more desirable, given that there is less scope to develop the law through the process of statutory interpretation by courts and others.

19.63 In assessing the merits of legislative amendment to the definition of consent, the ALRC has considered how consent has been dealt with in other pieces of federal legislation. Examples of expansion of the concept of consent in federal legislation appear in very specific circumstances. For example the:

---

89 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

90 See Chs 4, 18.

- *Crimes Act 1914* (Cth) sets out the steps that must be taken for informed consent to forensic procedures to be established.[91]

- *Criminal Code* (Cth) defines consent, in relation to sexual offences, as 'free and voluntary agreement' and sets out examples of circumstances in which a person does not consent to an act, such as where the person submits because of force, the fear of force or because the person is unlawfully detained.[92]

- *Spam Act 2003* (Cth) defines consent as express consent or consent that can be reasonably inferred from the conduct, and the business and other relationships, of the individual or organisation concerned.[93] It also defines consent in the specific context of sending an electronic message, in particular, the circumstances in which consent may be inferred from publication of an electronic address.[94]

19.64 Many other federal statutes which refer to consent, do not define it. Some provide that consent to entry of premises by an authorised person is not lawful unless the person *voluntarily* consents.[95]

19.65 The above survey highlights the fact that, while it may be possible to resort to legislation to define or explain consent in a particular context, providing a statutory definition that applies across a wide variety of contexts remains problematic.

Bundled consent

19.66 The parameters of the practice of bundled consent, and the circumstances in which it is appropriate to rely on such consent, needs to be clarified. Such clarification will provide greater protection for individuals and increased certainty for agencies and organisations.

19.67 It is apparent from views expressed to this Inquiry that agencies and organisations may abuse the practice of bundled consent. It is equally apparent, however, that there may be legitimate circumstances in which agencies and organisations may use and rely on bundled consent.

---

91 *Crimes Act 1914* (Cth) ss 23WF, 23WG, 23XWG.

92 *Criminal Code* (Cth) s 268.14 (Crime against humanity—rape); s 268.16 (Crime against humanity—enforced prostitution).

93 *Spam Act 2003* (Cth) sch 2 s 2.

94 Ibid sch 2.

95 See, eg, *Energy Efficiency Opportunities Act 2006* (Cth) s 31; *Fuel Quality Standards Act 2000* (Cth); *Renewable Energy (Electricity) Act 2000* (Cth) s 46, s 117; *Trade Practices Act 1974* (Cth) s 154D; *Migration Act 1958* (Cth) s 268CC; *Quarantine Act 1908* (Cth) s 66AW.

19.68 The OPC should develop and publish guidance on bundled consent. This guidance should address the practice of bundled consent in specific industry sectors, such as finance, debt collection, credit reporting, telecommunications, and residential tenancy. It should consider also the use of the practice when dealing with marginalised communities and in relation to the collection, use or disclosure of sensitive information. Finally, it is imperative that the OPC develops its guidance on consent, including bundled consent, in consultation with relevant stakeholders and industry sectors.

Recommendation 19–1 The Office of the Privacy Commissioner should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should:

(a) address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained;

(b) cover express and implied consent as it applies in various contexts; and

(c) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

A separate privacy principle dealing with consent?

Background

19.69 As noted above, consent is not a discrete privacy principle, although it plays a key role in the application of other privacy principles—namely those regulating the collection of sensitive information, use and disclosure, and cross-border data flows. While many jurisdictions do not deal separately with the concept of consent, some, like Canada and Germany,[96] elevate consent to a separate principle or provision. The Canadian *Model Code for the Protection of Personal Information*, for example, contains a principle, which provides:

> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[97]

96 *Federal Data Protection Act 1990* (Germany) s 4a.

97 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principle 4.3. Significantly, under the Canadian approach, consent is relevant to the collection of all personal information, not just sensitive information.

19.70 In Canada, the PIPED Act specifies a number of circumstances in which personal information can be collected, used and disclosed without a person's consent or knowledge.[98] The Model Code covers the form of the consent sought by the organisation, the manner in which an organisation can seek consent and in which an individual can give consent, and the withdrawal of consent by an individual.[99]

19.71 The draft Asia-Pacific Privacy Charter also contains a separate consent principle, which states:

> For some Principles, individual consent justifies actions that would otherwise not comply with the Principle. Where consent is relied upon, it must be freely-given, informed, variable and revocable. Consent is meaningless if people are not given full information, or have no option but to consent in order to obtain a benefit or service.
>
> For Principles where consent normally applies, there are exceptional situations where consent may be insufficient justification.[100]

Submissions and consultations

19.72 In response to IP 31, there was general opposition to the creation of a discrete privacy principle dealing with consent.[101] There was concern that this could be too onerous if it imposed additional obligations to obtain consent.[102]

19.73 AAMI submitted that, while there is not currently a discrete consent principle, it already 'exists by the very nature of what an organisation needs to do to collect and manage personal information'. A separate consent principle would therefore 'add no value'.[103] Moreover, a number of stakeholders submitted that it would be preferable to rely on the consent provisions in the existing privacy principles and to modify those provisions as necessary.[104]

19.74 In DP 72, the ALRC expressed the preliminary view that it would be inappropriate to create a discrete privacy principle dealing with consent.[105] This approach was supported by stakeholders, on the basis that such a creation was

---

98 Ibid s 7.

99 See Ibid sch 1, Principles 4.34, 4.36–4.38.

100 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 2.

101 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; AAMI, *Submission PR 147*, 29 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

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

103 AAMI, *Submission PR 147*, 29 January 2007.

104 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; AAMI, *Submission PR 147*, 29 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007.

105 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [16.43].

inappropriate, unnecessary, or would introduce greater complexity into privacy regulation.[106] No contrary views were expressed in this regard.

ALRC's view

19.75 It would be inappropriate to deal with consent as a discrete privacy principle. The concept of consent is built into the architecture of those privacy principles to which it is relevant. Such an approach emphasises that consent may have a role to play in various parts of the information cycle.

19.76 As noted above, consent is either framed as an exception to a general prohibition against personal information being treated in a particular way or as a basis to authorise the treatment of personal information in a particular way. Significantly, in each case, consent is not the only exception to a stated prohibition, or the only basis for permitting the treatment of personal information in a particular way. Treating consent as a separate privacy principle, therefore, may elevate consent to being the overriding factor in permitting or restricting the handling of personal information. In the ALRC's view this would not be appropriate. As Professor Fred Cate has stated:

> Requiring choice may be contrary to other activities important to society, such as national security or law enforcement, or to other values, such as freedom of communication. This explains why so many laws that purport to invest individuals with control over information about them exempt so many activities: it simply is not feasible or desirable to provide for individual control …[107]

19.77 Moreover, stakeholders have not identified any problems or issues arising from the location of consent within the privacy principles. Any radical change in this regard is not warranted.

---

106 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

107 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341, 342.

20. Anonymity and Pseudonymity

Contents

Introduction

20.1 This chapter concerns the principle of anonymity and pseudonymity. Currently, the *Privacy Act 1988* (Cth) provides a limited right for an individual to transact anonymously with organisations through National Privacy Principle (NPP) 8.[1] This right is designed to give individuals, where appropriate, greater control over how much personal information they wish to reveal to organisations with which they are dealing. Where applicable, it also allows an individual to reveal often intimate, personal information while minimising the risk that this information will be traced back to the individual concerned.

20.2 The anonymity principle complements NPP 1, which prohibits an organisation from collecting information that is not necessary for its functions or activities. In particular, NPP 8 is intended to affect the design of new technologies that collect more information than is necessary when an organisation transacts with individuals.[2]

20.3 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states:

> Anonymity is an important dimension of privacy. In some circumstances, it will not be practicable to do business anonymously. In others, there will be legal obligations

1 *Privacy Act 1988* (Cth) sch 3, NPP 8.
2 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5510].

> that require identification of the individual. Unless there is a good practical or legal reason to require identification, organisations should give people the option to operate anonymously. This principle is not intended to facilitate illegal activity.[3]

20.4 Some examples of where an individual may wish to transact anonymously with an agency or organisation include:

- making a telephone inquiry about a product or service; and
- using counselling services, especially where information is revealed about a third party.[4]

20.5 This chapter focuses on two main issues. The first is potential expansion of the anonymity principle under the model Unified Privacy Principles (UPPs), including: whether it should cover agencies in addition to organisations; and whether the principle should be expanded to cover pseudonymity. Secondly, the chapter considers what should be the content of this principle.

Expanding the anonymity principle

Expansion of anonymity principle to agencies

20.6 In accordance with NPP 8, wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[5] The Information Privacy Principles (IPPs), however, do not contain a comparable anonymity principle. Neither is such a provision set out in the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines), or in the privacy legislation of some jurisdictions, including New Zealand and the United Kingdom.[6] In contrast, German privacy law imposes obligations in relation to anonymity on both public and private sector bodies.[7] Similarly, Victorian, Tasmanian and Northern Territory privacy laws contain an anonymity principle that is applicable to public sector bodies.[8]

---

3 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [384].
4 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5520].
5 *Privacy Act 1988* (Cth) sch 3, NPP 8.
6 See *Privacy Act 1993* (NZ) s 6; *Data Protection Act 1998* (UK) sch 1.
7 See *Federal Data Protection Act 1990* (Germany) s 3a.
8 *Information Privacy Act 2000* (Vic) sch 1, IPP 8.1; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 8; *Information Act 2002* (NT) sch 2, IPP 8.

Submissions and consultations

20.7 In response to the Issues Paper, *Review of Privacy* (IP 31), a large number of stakeholders submitted that Commonwealth agencies should be subject to an anonymity principle.[9] The Office of the Privacy Commissioner (OPC), for example, commented that 'requiring individuals to be identifiable when it is not necessary can serve to limit the choice and control individuals have over their personal information'.[10] The OPC further noted that it could see 'no compelling argument or policy reason for not extending the anonymity principle to agencies'.[11]

20.8 In Discussion Paper 72, *Review of Australian Privacy Laws* (DP 72), the ALRC proposed that the anonymity principle should be expanded to cover both agencies and organisations.[12] A significant majority of stakeholders that commented on this issue supported the proposed extension.[13] Privacy NSW noted, for example, that the anonymity principle

> represents a logical step in minimising the collection of unnecessary personal information and gives individuals the opportunity to exercise a greater degree of control in relation to the collection, use and disclosure of their personal information.[14]

20.9 The OPC also commented favourably on the function of the anonymity principle as a way to 'encourage agencies and organisations to consider the fundamental question of whether they need to collect personal information at all'.[15]

20.10 Two agencies did not support the principle of extending anonymity requirements to agencies.[16] In addition, a number of agencies—although they did not

---

9 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Queensland Government, *Submission PR 242*, 15 March 2007; 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; K Pospisek, *Submission PR 104*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

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

11 Ibid.

12 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 17–1.

13 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; 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; 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.

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

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

16 Australian Federal Police, *Submission PR 545*, 24 December 2007; Confidential, *Submission PR 448*, 11 December 2007.

object to the proposed expansion—advised that they would have difficulties in applying the principle.[17] A small number of organisations also objected to any extensions to the present anonymity principle.[18]

20.11 Telstra commented that the proposed anonymity principle 'does not improve privacy protection in Australia and adds another level of complexity to an already complex compliance regime'.[19] It suggested that the 'Collection' principle, which requires organisations to collect only 'necessary' information, should provide sufficient assurance that organisations only collect a customer's personal information where it is appropriate to do so. One stakeholder suggested that anonymity requirements could be added to the 'Collection' principle, rather than forming the basis of a stand alone principle.[20]

20.12 The Cyberspace Law and Policy Centre submitted that the anonymity principle should be expanded further to impose an obligation on agencies and organisations to facilitate anonymous transactions with third parties.[21] This was illustrated through charging for unlisted telephone numbers. Although a customer of a telecommunications provider cannot remain anonymous from that provider, the Cyberspace Law and Policy Centre suggested that, as a part of the anonymity principle, he or she should be able to express a desire to remain anonymous at various stages of the provider's interaction with third parties—for example, the provision of information for directory assistance services.[22]

ALRC's view

20.13 The ALRC recommends that an anonymity principle should be included in the model UPPs and should apply equally to agencies and organisations. Providing the resulting privacy principle is appropriately worded, the ALRC considers that such an extension is desirable for a number of reasons.

---

17 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

18 BPay, *Submission PR 566*, 31 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

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

20 Confidential, *Submission PR 570*, 13 February 2008.

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

22 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007. See also, Australian Privacy Foundation, *Charging for Unlisted Numbers (Silent Lines)* (2006) <www.privacy.org.au/Papers/Silent-Line-v5.rtf> at 4 February 2008. The issue of charging for silent numbers is considered in Ch 72.

20.14 As noted by the OPC, an anonymity principle encourages agencies and organisations to consider the fundamental question of whether they need to collect personal information at all and to design their systems accordingly. Secondly, allowing individuals to retain greater control over their privacy by giving them the option to transact anonymously, where appropriate, will potentially give rise to significant public policy benefits. For example, this option might encourage an individual to seek medical or other assistance from an organisation or agency where, if the assistance was contingent on the individual identifying himself or herself, the individual would be discouraged from seeking the assistance. This can be illustrated by the anonymous supply of sterile syringes and needles to injecting drug users, which is an important public health initiative in all Australian states and territories. As well as face-to-face outlets, some needle and syringe programs include automatic dispensing machines, to accommodate people who wish to avoid interpersonal contact altogether.[23]

20.15 Agencies' concerns about the practical application of the principle can be accommodated adequately within the broader limitations of the principle—that is, that the option for anonymity must be provided only where it is 'lawful and practicable'. These requirements are discussed in more detail later in this chapter.

20.16 Only the Cyberspace Law and Policy Centre recommended the expansion of the principle to require agencies and organisations to facilitate anonymous transactions with third parties. The ALRC is concerned that such an expansion would be uncertain in its application and would place a potentially high compliance burden on agencies and organisations—for example, such an expansion may require significant modification of existing systems. This issue has to some extent been addressed through other recommendations in this Report that are directed towards the protection of third party information, for example, the recommendation that there should be no charge for silent telephone numbers.[24]

The concept of 'pseudonymity'

20.17 A further issue that was raised in this Inquiry is whether the concept of anonymity is too limited; in particular, whether the relevant privacy principle should be expanded specifically to include the concept of pseudonymity. Such an expansion would allow an individual to transact, subject to the relevant qualifications, pseudonymously with an agency or organisation. That would usually involve the individual providing an agency or organisation with a name, term or other combination of letters and numerals through which he or she can be addressed specifically. In this way, the individual may select a pseudonym that bears no relation to the individual's

---

23 See NSW Health, *Needle and Syringe Program Policy and Guidelines for NSW (PD 2006–037)* (2006). Automatic dispensing machines have also been trialled in Western Australia and the Australian Capital Territory.

24 Rec 72–17.

actual name, as occurs commonly with internet usernames. There is an example of this approach in the *Federal Data Protection Act 1990* (Germany).

> The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and pseudonymisation where possible and where the effort entailed is proportionate to the interests sought to be protected. [25]

Submissions and consultations

20.18 In DP 72, the ALRC came to the preliminary view that the proposed UPPs should enable, where appropriate, an individual to transact pseudonymously as well as anonymously, with an agency or organisation.[26] This provision was considered to be useful, particularly in the online environment.[27]

20.19 The majority of stakeholders that commented on this issue welcomed the proposal to extend the anonymity principle to include pseudonymity.[28] The Public Interest Advocacy Centre (PIAC), for example, noted that:

> Complete anonymity will not always be possible because an agency or organisation may need to have some means of differentiating between individuals. Pseudonymity provides a practical alternative in situations where the agency or organisation needs to be able to differentiate, but does not need to know the name and other personal details of the individual.[29]

20.20 Similarly, the Office of the Victorian Privacy Commissioner (OVPC) commented that,

> in situations where it is necessary to determine that the individual involved in a particular transaction is the same one as has been involved in previous transactions, without actually identifying the individual, pseudonymity is a desirable option.[30]

20.21 A smaller number of stakeholders raised theoretical and practical problems with the inclusion of a pseudonymity requirement.[31] Some of these stakeholders considered that pseudonymous transactions were open to abuse and may detract from the accuracy

---

25 *Federal Data Protection Act 1990* (Germany) s 3(6a).

26 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 17–2.

27 Ibid, [17.20].

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

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

30 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

31 BPay, *Submission PR 566*, 31 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

of information.[32] Stakeholders also suggested that pseudonymity would provide little additional benefit to anonymity.[33] For example, it was submitted that,

> where it is not necessary for an organisation or agency to take any record in relation to a transaction, anonymity is normally practicable and lawful. Where a record does need to be made, for legal or practical purposes, it would in most circumstances be highly inappropriate that the record be made under a pseudonym.[34]

20.22 The Law Council of Australia noted that an extension to a pseudonymity requirement will require organisations and agencies to review their methods of transacting with individuals.

> Given the pseudonymity requirement is a novel concept, it is highly unlikely that many agencies or organisations will have processes to accommodate this. Implementation could well be difficult, time consuming and expensive.[35]

20.23 Although it supported the inclusion of pseudonymity within the anonymity principle, the OPC raised concerns that agencies and organisations may use the terms pseudonymity and anonymity interchangeably and thereby only offer one of the options to individuals. It suggested that this could have the effect of reducing an individual's choice over the manner in which he or she interacts with agencies and organisations. The OPC further noted the possibility that information collected in a pseudonymous transaction could, in some circumstances, amount to personal information. This would be the case, for example, where a new technology enables an organisation or agency to use information provided by an individual under a pseudonymous transaction to identify the individual.[36]

20.24 The OPC suggested

> that the wording of the principle [should] be clarified to ensure that organisations and agencies provide individuals with the option of interacting anonymously where this is lawful and practicable. Where it is not practicable for an individual to transact anonymously or where the individual chooses to transact under a pseudonym an agency or organisation [should be] required to give individuals the clear option to transact pseudonymously if this is lawful and practicable.[37]

---

32 Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

33 BPay, *Submission PR 566*, 31 January 2008; Confidential, *Submission PR 536*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

34 Confidential, *Submission PR 536*, 21 December 2007.

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

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

37 Ibid.

ALRC's view

20.25 The ALRC recommends that the anonymity principle should provide for pseudonymous transactions. This provides a more flexible application of the principle, by covering the situation where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation. An extension of the principle to encompass pseudonymous transactions will also encourage agencies and organisations to incorporate into their systems privacy-enhancing technologies that facilitate pseudonymous interactions in an online environment.[38]

20.26 Two principal objections to a pseudonymity requirement were raised in submissions: the cost of implementation, particularly where it would have a relatively limited application; and the potential to detract from the accuracy of records. These issues can be accommodated adequately within the broader limitations of the 'Anonymity and Pseudonymity' principle—that is, transacting anonymously or pseudonymously must be 'lawful and practicable'. These requirements are discussed in more detail later in this chapter.

20.27 Depending on the amount of information collected and the nature of such information, it is possible that information collected under a pseudonym could fall (either at the time of collection or at some stage in the future) within the definition of 'personal information'. The ALRC is not convinced, however, that the principle itself needs to 'rank' expressly the options of anonymity and pseudonymity. Rather, the decision of an agency or organisation to provide an option to interact anonymously or pseudonymously will be guided by the particular context. Generally speaking, where the agency or organisation has no need to contact the individual in the future, anonymity would be the most appropriate option. Where some form of identifier is required but need not be personal information, pseudonymity is likely to be appropriate. The relevant matters that an agency or organisation should address when considering whether to provide an option for anonymity or pseudonymity can appropriately be dealt with in guidance on the principle.

Application of the 'Anonymity and Pseudonymity' principle

'Lawful and practicable'

20.28 The requirement to provide the option for anonymity or pseudonymity is not absolute. In particular, under NPP 8, organisations are required to provide individuals with the option of not identifying themselves only where it is 'lawful and practicable'. NPP 8 is also limited to situations where individuals are 'entering into transactions' with an organisation.

---

38 See the detailed discussion on privacy and developing technology in Part B.

20.29 Some factors that agencies or organisations should consider when determining whether it is practicable to deal with an individual anonymously or pseudonymously include whether:

- the provision of the product or service requires the individual to be identified;
- the provision of the product or service could be improved if the individual was known;
- there will be an increase in cost or time involved in providing the service; and
- there will be an increased risk to the organisation or agency in providing the service anonymously or pseudonymously, for example in the event of legal proceedings.[39]

20.30 It may not be lawful for an agency or organisation to provide the option of anonymity or pseudonymity where the agency or organisation is required to collect identifying information; for example, for the purpose of mandatory reporting requirements including notifiable diseases or suspected child abuse, or opening a bank account.[40] In DP 72, the ALRC also suggested that the requirement of 'lawful' would not be met where the failure to collect the identifying information by the agency or organisation would result in the individual acting unlawfully, for example where an individual wishes to transact anonymously in order to further a fraudulent conspiracy of which the individual is a part.[41]

20.31 In DP 72, the ALRC also proposed an additional clarification of the 'Anonymity and Pseudonymity' principle, which was replacing the words 'when entering transactions' in the current NPP 8 with the words 'when transacting'.[42] This was intended to make it clear that where an individual has an existing relationship with an agency or organisation that individual is still entitled to transact anonymously.[43]

Submissions and consultations

20.32 A large number of agencies and organisations expressed concerns that the practical application of the 'Anonymity and Pseudonymity' principle would interfere with their functions.[44] In particular, concerns were raised by agencies involved in

---

39 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5500].
40 Ibid, [2-5530].
41 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [17.18].
42 Ibid, Proposal 17–2.
43 Ibid, [17.24]–[17.25].
44 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008; Australian Government Department of Human Services,

service delivery.[45] The Department of Disability Housing and Community Services (ACT), for example, advised that:

> The Office for Children, Youth and Family Support (OCYFS) provides services to children and young people … including to children at risk of abuse or neglect. Accurate identification of names assists in the provision of appropriate recording of client history (which assists with risk assessment) and is essential at times for assisting with the procurement of services for children on care orders who require financial assistance for medical services and other such items.[46]

20.33 Similarly, the Australian Government Department of Human Services advised that it cannot provide full and reliable advice to an individual that remains anonymous or provides a pseudonym. This advice requires a full discussion of his or her circumstances.[47]

20.34 The Department of Foreign Affairs and Trade expressed concern about the potential compliance burden of providing individuals with the option to transact pseudonymously, for example by requiring amendment of the Department's online forms such as passport applications.[48] The Law Council of Australia also submitted that a requirement to provide an option of pseudonymity could be time consuming and expensive.[49]

20.35 Stakeholders also identified a range of situations where the application of the 'Anonymity and Pseudonymity' principle could conflict with legislative requirements on the organisation to retain identifying information. Examples included legislative requirements that apply to the telecommunications industry,[50] the provision of health care[51] and health insurance[52] and the financial services sector.[53]

Submission PR 541, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 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; Queensland Government, *Submission PR 490*, 19 December 2007.

45 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

46 ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007.

47 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

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

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

50 Optus, *Submission PR 532*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. Telecommunications issues are discussed further in Part J.

51 Australian Medical Association, *Submission PR 524*, 21 December 2007.

52 BUPA Australia Health, *Submission PR 455*, 7 December 2007.

53 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

20.36 Some stakeholders suggested that a specific exception should be provided from the 'Anonymity and Pseudonymity' principle, for example, for the delivery of health benefits and social services by Commonwealth agencies,[54] or for the provision of health care.[55]

20.37 Other stakeholders expressed concerns about the potential for an agency or organisation to rely upon the requirement that anonymous or pseudonymous transactions should be 'practicable' to evade its obligations under this principle.[56] In particular, they noted that options for anonymity or pseudonymity should be considered at the design stage of new information systems to prevent impracticality being relied upon further down the track. They suggested, therefore, that the principle should provide expressly that the obligation for organisations and agencies applies at the stage when an information system is being designed, as well as the time that an individual enters into a transaction with an agency or organisation.[57]

20.38 The Cyberspace Law and Policy Centre, for example, used the example of cashless toll roads to illustrate the need for anonymity and pseudonymity options to be integrated into information systems.

> The opportunity for anonymous travel has been removed by the removal of cash booths and the choice of tolling systems and business models that require vehicles (and their registered owners) to be identified. Had sufficient attention been paid to an anonymity/pseudonymity principle at the outset, it should have been possible to design automated toll roads that either respected the right of anonymous travel (through the use of pre-paid debit tags) or at least offered 'pseudonymous' accounts where identification of the actual user would only be triggered by exceptional events, (such as non-payment, accidents or crime).[58]

20.39 The Cyberspace Law and Policy Centre also advised that the potential for isolated cases of abuse should not be sufficient to make the option for anonymity or pseudonymity 'unlawful'. Rather than assessing the intentions of each individual, it argued that agencies and organisations should undertake a high level assessment of risk.[59]

> It is impossible to know in advance the motives of an individual in seeking anonymity or using a pseudonym. Any system can and will be abused in isolated cases—and that alone is not sufficient justification for exemption from this principle. It would only be reasonable to decline to provide anonymous or pseudonymous option where an

---

54 Australian Government Department of Human Services, *Submission PR 541,* 21 December 2007.

55 Australian Medical Association, *Submission PR 524,* 21 December 2007.

56 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.

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

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

59 Ibid.

overall assessment of the resulting risk of fraud or other unlawful behaviour was both high and widespread—i.e. where it was likely to be abused by many individuals.[60]

Options for reform

20.40 A number of options for reform of the 'Anonymity and Pseudonymity' principle were supported in submissions, including:

- replacing the word 'transact' with 'interact', to clarify that the obligation applies before any sale or contract, which is when it is likely to have the most relevance;[61]

- introducing specific exceptions for the delivery of health benefits and social services by Commonwealth agencies,[62] and for the provision of health care;[63] and

- additional guidance on the application of the principle, including on how the principle should be balanced with other obligations of the agency or organisation.[64]

ALRC's view

20.41 The 'Anonymity and Pseudonymity' principle is an important component of the model UPPs. Agencies and organisations, however, expressed widespread concerns about its practical application. The best way of addressing these concerns is by clarifying the types of dealings where the principle is likely to apply.

20.42 One way of clarifying the application of the principle is by replacing the word 'transacting' with 'interacting'. Since, on its plain English meaning, 'interact' is a word of wider import than 'transact', this more clearly establishes the broad spectrum of dealings between individuals and agencies or organisations where identifying information may not be required. The term 'transacting' may be associated unduly with customised transactions or service delivery, where anonymity or pseudonymity will often not be appropriate.

20.43 There is also a need for additional certainty concerning the requirements of 'lawful and practicable', including:

- an agency's or organisation's application of the 'practicable' requirement when delivering a service to an individual or entering into a customised transaction;

---

60 Ibid.
61 Confidential, *Submission PR 536*, 21 December 2007.
62 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.
63 Australian Medical Association, *Submission PR 524*, 21 December 2007.
64 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

- the factors an agency or organisation should take into account when it balances the requirement that it should provide individuals with the option to interact anonymously or pseudonymously wherever it is 'practicable' to do so with the compliance burden of providing this option; and

- the extent to which 'lawful' extends to an agency or organisation that, by providing an option to interact anonymously or pseudonymously, facilitates unlawful actions on the part of the individual.

20.44 The OPC should issue guidance on the 'Anonymity and Pseudonymity' principle—including on the interpretation of the requirements of 'lawful and practicable'.

20.45 Another way that agencies and organisations can accommodate the 'Anonymity and Pseudonymity' principle is through their Privacy Policy.[65] This document could include, for example, information on the interactions for which anonymity or pseudonymity is available, including any consequences for an individual that chooses to take up such an option. For example, a complaint-handling program may allow complaints to be received in an identified or anonymous form. Where an identified complaint is made, follow-up information can be provided to the complainant on the outcome of the complaint or steps being taken to rectify the situation. Where an anonymous complaint is received, this follow up will not be possible. By setting out these trade-offs up front, an agency or organisation provides an individual with the opportunity to decide which interests take precedence.

20.46 The reforms set out above will accommodate adequately the application of the 'Anonymity and Pseudonymity' principle by a diverse spectrum of agencies and organisations. Therefore, specific agencies or organisations should not be granted an exception from the principle. Rather, the question of whether the principle should apply will depend on the nature of the particular interaction. For example, where an agency is undertaking an activity that is directly connected to the provision of a government benefit, it generally will not be 'lawful and practicable' for the agency to offer an option of anonymity or pseudonymity. Where the agency is undertaking a more generic interaction, however, such as providing advice on general departmental policy or procedure, anonymity or pseudonymity may be appropriate.

20.47 Focusing the application of the principle on the nature of the particular interaction is also supported by submissions from a number of agencies and organisations involved in service delivery, which identified functions that they carry out that are already undertaken anonymously, or could in the future potentially be undertaken anonymously.

---

65 Privacy Policies are discussed in Ch 24.

'Not misleading'

20.48 In DP 72, the ALRC noted the potential for pseudonymous transactions to lead to a risk of fraud or misleading practices. Although the ALRC suggested that fraud was adequately covered by the requirement that the transaction be 'lawful', it was concerned that in some circumstances it may be misleading—even where not necessarily fraudulent—for an individual to provide a pseudonym, or particular types of pseudonym. This can be illustrated by a situation where an individual deliberately chooses as a pseudonym someone else's name in order to give the impression that he or she is actually that other person.

20.49 In order to minimise the potential for such practices, the ALRC proposed that the option to transact pseudonymously should be subject to the additional limitation of situations where it would not be misleading.[66]

Submissions and consultations

20.50 In submissions on DP 72, some stakeholders objected to the inclusion of a pseudonymity-specific requirement that the use of the pseudonym not be misleading.[67] In particular, concerns were raised that this requirement was an oxymoron—that is, that the very nature of a pseudonym is to mislead as to identity.[68]

20.51 The Cyberspace Law and Policy Centre, for instance, suggested that the qualification 'where lawful and practicable' should cover all the necessary exceptions. It noted that the example provided by the ALRC in this context—a person using another individual's name as his or her pseudonym—would either be fraudulent (where there was an intention to impersonate) or harmless and unobjectionable (such as using a celebrity's name in fun). It also submitted that organisations and agencies are not equipped to assess an individual's intentions when he or she interacts pseudonymously.[69]

20.52 The OVPC advised that the practical application of this requirement could be difficult, submitting that,

> careful thought and guidance will need to be provided by Privacy Commissioners in relation to the meaning of 'not misleading' as there is potential for agencies and organisations to interpret this phrase broadly and thus to deny individuals the

66 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 17–2. See also Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [17.23].

67 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.

68 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.

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

> opportunity to transact pseudonymously, even where there is no genuine need to identify the individual concerned.[70]

20.53 Some stakeholders suggested alternative wordings for a pseudonymity-specific requirement; for example, pseudonyms that are 'not likely to cause any material loss or damage to any person',[71] or wording to make it clear that pseudonyms 'cannot be used with deliberate intent to commit fraud or deliberately pass oneself off as another real person'.[72] RCSA suggested that, in addition to the requirement that a pseudonym be 'not misleading', it should also not be 'offensive'.[73]

ALRC's view

20.54 The ALRC accepts that there is the potential for pseudonymous interactions to result in misleading practices; in particular, where an individual deliberately passes himself or herself off as another real person. For example, an online news site may provide for pseudonymous comments to be posted on articles. An individual could post comments on articles under a pseudonym that has been selected deliberately in order to mislead other readers into believing that the posts have been made by someone else. Depending on the circumstances, this could result in loss or damage to the individual impersonated and to the news site.

20.55 The ALRC also accepts the inherently misleading nature of pseudonyms. As one commentator has noted, 'except where unavoidable, a user's online presence will generally contain some level of falsification'.[74] The ALRC agrees that a requirement that a pseudonym not be misleading could be difficult for agencies and organisations to apply.

20.56 The requirement that the pseudonymous interaction must be 'lawful and practicable' is sufficient to guard against systemic abuse. The ALRC also notes that the pseudonymity provision in the German *Federal Data Protection Act*—at present, the only example of a pseudonymity provision that has been incorporated into privacy legislation—does not include a limitation that the interaction not be misleading. Rather, it requires that use be made of the options of anonymity and pseudonymity 'where possible' and where it is proportionate to the interests sought to be protected.[75]

---

70 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
71 Law Council of Australia, *Submission PR 527*, 21 December 2007.
72 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
73 Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.
74 A Sauer, 'Online Privacy and the Online Self', *Lawyers Weekly*, 25 January 2008, 24.
75 *Federal Data Protection Act 1990* (Germany) s 3a.

The onus on agencies and organisations

20.57 In DP 72, the ALRC proposed that agencies and organisations be required to give individuals the *clear* option of transacting anonymously or pseudonymously. In doing this, it distinguished between an obligation to provide an *express* option to individuals and an obligation to provide a *clear* option. An express option would require an agency or organisation to state explicitly (for example, on its information collecting system) that individuals may transact anonymously or pseudonymously. A clear option, however, was considered to be less prescriptive and merely requires that the agency or organisation ensure that individuals are aware that they may transact anonymously or pseudonymously.

20.58 A requirement to provide individuals with a clear option would be less onerous and cumbersome, in most instances, than a requirement to provide an express option. It would allow agencies and organisations to comply with the 'Anonymity and Pseudonymity' principle in the *structure* of their information collecting systems. For example, in many cases where asked to fill out a form either on paper or electronically, individuals are told which fields they must complete.[76] Providing a clear option may entail altering the list of 'required fields' to take account of the 'Anonymity and Pseudonymity' principle. An express option may require agencies and organisations to undertake an additional step of notifying individuals that they do not need to complete the fields containing identifying information.

Submissions and consultations

20.59 The overwhelming majority of stakeholders that commented on this issue supported the ALRC's formulation of a clear option.[77] A small number of stakeholders did not support the proposed formulation.[78] Telstra, for example, submitted that providing customers with a clear option to transact anonymously or pseudonymously 'would add to an already heavy compliance burden for organisations'.[79]

20.60 The OVPC suggested that there may be some situations where an organisation or agency should turn its mind to whether expressly providing the option to remain anonymous or pseudonymous (if lawful and practicable) is preferable to providing a

---

76 A 'field', on a form, is the space reserved for an individual to provide his or her response to a question that is asked on the form.

77 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; 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.

78 BPay, *Submission PR 566*, 31 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

79 Telstra Corporation Limited, *Submission PR 459*, 11 December 2007. See also BPay, *Submission PR 566*, 31 January 2008.

clear option.[80] Medicare Australia submitted that a clear option needs to be qualified to include only circumstances where it is a valid option.[81]

20.61 A related issue that was raised in some submissions is whether the 'Anonymity and Pseudonymity' principle should be redrafted to place a more active responsibility on agencies and organisations to provide individuals with the option of interacting anonymously or pseudonymously.[82] The Public Interest Advocacy Centre (PIAC), for example, submitted that this could involve redrafting the principle along the lines of the Northern Territory's anonymity principle,[83] which states that 'a public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself'.[84] Some stakeholders suggested that this would more closely align the 'Anonymity and Pseudonymity' principle with the drafting of the other UPPs[85] and better reflect the wording of the proposals on which the principle is based.[86]

ALRC's view

20.62 Requiring agencies and organisations to provide individuals with a clear option of interacting anonymously or pseudonymously represents an appropriate balance between the interest in making individuals aware of their option to not identify themselves, or identify themselves pseudonymously, and the need to limit the cost of compliance for agencies and organisations. The formulation of a clear option was also supported by the majority of stakeholders.

20.63 The concerns that agencies and organisations put forward—in particular, the potential compliance burden associated with this recommendation—will be accommodated adequately by the requirement that the option be 'lawful and practicable'. For example, where providing a clear option for an individual to transact anonymously or pseudonymously would require an agency or organisation to make substantial and costly *changes* to its systems, generally this would not be considered 'practicable'. The principle would require agencies and organisations, however, to consider the possibility of such an option in the *design* of their systems.

---

80 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

82 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.

83 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

84 *Information Act 2002* (NT) sch 2, IPP 8.

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

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

20.64 The ALRC agrees with the suggestion that the 'Anonymity and Pseudonymity' principle should be redrafted to clarify that the onus is on agencies and organisations to give individuals options to interact anonymously and pseudonymously. That is, rather than the formulation proposed in DP 72—that, in the relevant circumstances, 'individuals should have the option of not identifying themselves' when transacting with an agency or organisation[87]—the model UPP should be drafted as follows: 'Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of either: (a) not identifying themselves; or (b) identifying themselves with a pseudonym'.

20.65 There are two primary benefits to redrafting the principle in this way. First, it sets out clearly that agencies and organisations must take active steps to provide individuals with the option to interact anonymously or pseudonymously. Secondly, it is consistent with the phrasing of the other model UPPs. The principle remains qualified by the limitations of lawfulness and practicability.

Recommendation 20–1 The model Unified Privacy Principles should contain a principle called 'Anonymity and Pseudonymity' that requires an agency or organisation to give individuals the clear option to interact anonymously or pseudonymously, where this is lawful and practicable in the circumstances.

Guidance on the 'Anonymity and Pseudonymity' principle

20.66 In DP 72, the ALRC proposed that the OPC should provide guidance to agencies and organisations on the 'Anonymity and Pseudonymity' principle. Such guidance could cover: when it is and is not lawful and practicable to give individuals the option to transact anonymously or pseudonymously; when it would be misleading for an individual to transact pseudonymously with an agency or organisation; and what is involved in providing a clear option to transact anonymously or pseudonymously.[88]

20.67 The proposal for OPC guidance received significant support from stakeholders.[89] Some stakeholders, however, suggested that the OPC should be

87 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), UPP 1. This was adapted from the drafting of NPP 8.

88 Ibid, Proposal 17–4.

89 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

required to consult with relevant stakeholders when preparing this guidance.[90] For example, the Department of Human Services submitted that the OPC should consult with the Department and its agencies to ensure that the guidance takes into account the nature of Departmental business and the operations of service delivery agencies.[91] Similarly, Optus recommended that the OPC consult with affected businesses to ensure that significant compliance costs do not arise from actions taken to comply with this guidance.[92]

20.68 A small number of stakeholders did not support the proposal for OPC guidance.[93] GE Money, for example, did not agree that the OPC should issue guidance on when it is and is not lawful and practicable to permit an individual to transact with it anonymously or pseudonymously.[94] It submitted that these considerations will depend on a range of different obligations on organisations to identify their customers, such as anti-money laundering legislation. These primarily will not be requirements under privacy laws.[95]

ALRC's view

20.69 Guidance from the OPC will be integral to the application of the 'Anonymity and Pseudonymity' principle. In particular, this guidance will assist agencies and organisations to assess the types of interactions where anonymous and pseudonymous options are suitable. Such guidance also will help to clarify the factors an agency or organisation should take into account when determining whether the balance between the requirement that the option be 'practicable' and the potential compliance burden that implementation of such an option would have on agencies and organisations has been met.

20.70 The ALRC agrees that some industry sectors will have particular obligations that the OPC should take into account when it is developing guidance on the application of the 'Anonymity and Pseudonymity' principle. These may include those agencies and organisations that are subject to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and agencies involved in service delivery. The Privacy Commissioner is required, in performing his or her functions, to recognise 'the right of government and business to achieve their objectives in an efficient way'.[96] In

---

90 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.

91 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

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

93 BPay, *Submission PR 566*, 31 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007.

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

95 Ibid.

96 *Privacy Act 1988* (Cth) s 29(a).

some situations, the OPC's compliance with this objective will include consulting with affected agencies and organisations when it develops guidance.[97]

Recommendation 20–2 The Office of the Privacy Commissioner should develop and publish guidance on:

(a) when it is and is not 'lawful and practicable' to give individuals the option to interact anonymously or pseudonymously with agencies or organisations;

(b) what is involved in providing a 'clear option' to interact anonymously or pseudonymously; and

(c) the difference between providing individuals with the option to interact anonymously and pseudonymously.

Summary of 'Anonymity and Pseudonymity' principle

20.71 The first principle in the model UPPs should be called 'Anonymity and Pseudonymity'. It may be summarised as follows.

UPP 1. Anonymity and Pseudonymity

Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:

(a) not identifying themselves; or

(b) identifying themselves with a pseudonym.

97 The Office of the Privacy Commissioner is discussed in Part F.

21. Collection

Contents

Introduction

21.1 The collection of personal information, including the receipt and retention of unsolicited personal information, marks the initial stage in the information cycle. Without collection, issues concerning use; disclosure; access; correction; and cross-border data flows do not arise. It is therefore important for the collection of personal information to be regulated appropriately.

21.2 The privacy principles in the *Privacy Act 1988* (Cth) impose restrictions on the collection of personal information by agencies and organisations. Similar but different requirements are imposed on the public and private sectors. This chapter considers how the principles currently regulate the collection of personal information. It also considers the limitations that should be placed by the model Unified Privacy Principles (UPPs) on the collection of personal information and, in particular, how agencies and organisations should deal with unsolicited personal information.

Current coverage by IPPs and NPPs

21.3 Significantly, neither the Information Privacy Principles (IPPs) nor the National Privacy Principles (NPPs) require that an individual give his or her consent before an agency or organisation is permitted to collect the individual's personal information. There is, however, a general prohibition, subject to a finite list of exceptions, against the collection of sensitive information by organisations. One of these exceptions is where the individual consents to the collection.[1]

21.4 IPPs 1–3 deal with the collection of personal information by government agencies. IPP 1 provides that personal information shall not be collected for inclusion in a 'record' or in a 'generally available publication' unless: (a) the purpose for which the information is collected is lawful and directly related to a function or activity of the collector; and (b) the collection is necessary for, or directly related to, that purpose. The Office of the Privacy Commissioner (OPC) has expressed the view that 'purpose of collection' is to be interpreted narrowly, and that agencies should have a clear purpose for collecting each piece of personal information. It is not generally acceptable for an agency to collect information just because it may be useful in the future.[2] In addition, IPP 1 provides that personal information is not to be collected by unlawful or unfair means.

21.5 IPPs 2 and 3 cover 'solicitation' of personal information. IPP 2 provides that where an agency solicits personal information directly from the individual concerned for inclusion in a record or a generally available publication, the agency must take reasonable steps to ensure that, before or soon after the information is collected, the individual is generally aware of:

- the purpose for which the information is being collected;
- if applicable, the fact that the collection is authorised or required by law; and
- to whom it is the agency's usual practice to disclose or pass on personal information of the kind collected.

21.6 The Explanatory Memorandum notes that there would be circumstances in which an agency would not need to take any steps to ensure that the individual was aware of the matters specified in IPP 2 when soliciting personal information from that person.[3]

---

1 *Privacy Act 1988* (Cth) sch 3, NPP 10.1(a).

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

3 See Explanatory Memorandum, Privacy Bill 1988 (Cth), [61].

21.7 IPP 3 provides that where an agency solicits personal information for inclusion in a record or in a generally available publication, it must take reasonable steps, having regard to the purpose for which the information is collected, to ensure that the:

- information is relevant to that purpose, up-to-date and complete; and
- collection does not intrude unreasonably on the individual's personal affairs.

21.8 This principle is limited to personal information solicited from the individual and from third parties. It does not extend to information received without solicitation by the agency.[4]

21.9 NPP 1 provides that an organisation may only collect personal information:

- that is necessary for one or more of its functions or activities;
- by lawful and fair means and not in an unreasonably intrusive manner;
- after taking reasonable steps to ensure the individual is aware of: the organisation's identity and contact details; the fact that he or she can access the information; the purposes of collection; the organisations to which the organisation usually discloses information of that kind; any law requiring the particular information to be collected; and the main consequences for the individual if the information is not provided; and
- from the individual to whom the information relates if it is reasonable and practicable to do so, or from someone else if it takes reasonable steps to ensure that the individual is aware of the matters listed above, except to the extent that making the individual aware would pose a serious threat to anyone's life or health.

21.10 Further restrictions apply to the collection of sensitive information. These are set out in NPP 10, and discussed separately in Chapter 22.[5]

Collection from the individual

Background

21.11 NPP 1 obliges an organisation, where reasonable and practicable, to collect personal information about an individual *only* from that individual. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000

4 Ibid, [63].
5 'Sensitive information', which is a subset of personal information, is defined in s 6(1) of the *Privacy Act*.

acknowledges that there will be situations in which it would not be 'reasonable and practicable' to collect directly from an individual. It states that:

> An example would be where direct collection would prejudice the purpose of collection (eg in the case where an enforcement body is investigating a breach of a criminal law).[6]

21.12 The OPC has issued guidance on this principle, which sets out the following factors to be balanced in assessing whether it is reasonable and practicable to collect information directly from an individual:

- whether it is possible to collect the information directly;
- whether a reasonable individual might expect information about him or her to be collected directly or indirectly;
- how sensitive the information is;
- the cost to an organisation of collecting directly rather than indirectly;
- the privacy consequences for the individual if the information is collected indirectly; and
- what is accepted practice (by consumers and the industry).[7]

21.13 IPPs 1–3 do not impose an equivalent requirement on agencies to collect information directly from an individual where reasonable and practicable.

21.14 There is precedent in other jurisdictions for requiring agencies, where reasonable, only to collect personal information from the individual concerned. In New South Wales, for example, such an obligation applies to agencies unless the individual concerned has authorised collection from someone else or, where the information relates to a person under the age of 16, the information has been provided by a parent or guardian.[8] Privacy laws in New Zealand and Germany require agencies to collect personal information directly from the individuals concerned, except in certain specified circumstances, such as where:

- the administrative task to be fulfilled by its nature or purpose makes collection from other persons or bodies necessary;[9]
- non-compliance would not prejudice the interests of the individual concerned;[10]

---

6 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [337].

7 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 31–32.

8 *Privacy and Personal Information Protection Act 1998* (NSW) s 9.

9 *Federal Data Protection Act 1990* (Germany) s 4(2)(a).

10 *Privacy Act 1993* (NZ) s 6, IPP 2(c).

- non-compliance is necessary to avoid prejudice to the maintenance of the law … including the prevention, detection, investigation, prosecution, and punishment of offences; or
- compliance would prejudice the purpose of the collection.[11]

21.15 Privacy laws in Canada require a government institution, where possible, to collect personal information that it intends to use for an administrative purpose directly from the individual to whom it relates except in certain specified circumstances.[12] Similarly, United States law requires agencies to

> collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.[13]

Submissions and consultations

21.16 In the Issues Paper, *Review of Privacy* (IP 31) the ALRC asked whether agencies also should be subject to a general requirement that, where reasonable and practicable, they should collect information about an individual only from the individual concerned.[14]

21.17 Some stakeholders expressed the view that agencies should be subject to such a requirement, stating that there is no reason to retain different rules for agencies and organisations in these circumstances.[15] Some stakeholders emphasised that the requirement should apply only where reasonable and practicable, and that collection should not be jeopardised when it is not reasonable or practicable to obtain the information from the individual.[16]

---

11 Ibid s 6, IPP 2(e).

12 See *Privacy Act* RS 1985, c P-21 (Canada) s 5(1); *Privacy Act 1993* (NZ) s 6, IPP 2; *Federal Data Protection Act 1990* (Germany) s 4(2).

13 See *Privacy Act 1974* 5 USC § 552a (US).

14 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–3.

15 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; 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; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007.

16 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Queensland Government, *Submission PR 242*, 15 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Australian Competition and Consumer Commission, *Submission PR 178*, 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; 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.

21.18 Other stakeholders, however, opposed the imposition of this requirement.[17] For example, the Australian Federal Police (AFP) stated that law enforcement agencies routinely collect personal information from a range of sources, and that a 'reasonable and practicable test may not be sensitive enough to recognise this and may have significant operational impacts'.[18] The Australian Government Department of Families, Community Services and Indigenous Affairs (FaCSIA) submitted that such a requirement would hamper agencies' whole of government approach to service delivery because:

> Requiring each agency to separately collect information from the individual for the same programme would lead to a duplication of process and increase administrative inefficiency of government agencies.[19]

21.19 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the:

- UPPs should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information only from the individual concerned; and

- OPC should provide guidance to clarify when it would not be reasonable and practicable to collect such information from the individual concerned.[20]

21.20 Many stakeholders supported this proposal.[21] Reasons given for supporting direct collection of personal information from the individual concerned include that it gives individuals 'an opportunity to refuse to participate in the collection or provide their information on conditions' and increases the likelihood that the information collected will be relevant, accurate and complete.[22]

---

17 Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Taxation Office, *Submission PR 168*, 15 February 2007; Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007; Confidential, *Submission PR 165*, 1 February 2007.

18 Australian Federal Police, *Submission PR 186*, 9 February 2007. See also Confidential, *Submission PR 165*, 1 February 2007.

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

20 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 18–1.

21 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; 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; 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. One stakeholder submitted that it did not disagree with this approach: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

22 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

21.21 Some stakeholders that supported the proposal emphasised that there will be many cases where it will be necessary to obtain personal information from sources other than the individual concerned, and that guidance should address these circumstances.[23] For example, the National Health and Medical Research Council (NHMRC) noted that such circumstances include the taking of family, medical or social histories and the collection of information provided in confidence by third parties to health care providers.[24] The Department of Foreign Affairs and Trade submitted that it regularly collects personal information about individuals from third parties.

> For example, personal information is collected from next of kin and foreign authorities when dealing with consular cases; from other agencies, both state and Commonwealth, when establishing a passport applicant's identity and citizenship or conducting fraud investigations; from other employees when undertaking Code of Conduct and other internal investigations; and from a range of sources when processing security clearances for potential employees. It is assumed that each of these collections would fall within the 'reasonable and practicable' limitation … Guidance from the OPC to this effect would be necessary if this recommendation is adopted.[25]

21.22 Similarly, the Department of Defence welcomed guidance from the OPC on the parameters of what is 'reasonable and practicable'. It stated such guidance should not inhibit its ability to collect personal information about an individual's family and friends for the purposes of identity process checks and security clearance assessments.[26]

21.23 Stakeholders suggested also that the OPC's guidance cover collection:

- from persons authorised to act on behalf of the individual, such as parents and guardians;[27]
- from children and persons with a decision-making impairment;[28]

---

23 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Medicare Australia, *Submission PR 534*, 21 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

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

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

26 Australian Government Department of Defence, *Submission PR 440*, 10 December 2007. Another stakeholder noted that it would be impracticable to obtain information directly from an individual in the context of considering the promotion of servicemen, in matters relating to discipline, and investigations of wrongdoing, offences and breaches of security: D Meehan, *Submission PR 345*, 22 November 2007.

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

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

- processes which will gather information about multiple individuals, such as family support services and counselling;[29]

- for the purposes of investigations by agencies and organisations.[30]

21.24 Some stakeholders supported the proposal, subject to general reservations about the value of OPC guidance based, in part, on its non-binding nature.[31] Stakeholders emphasised the importance of OPC guidance being developed in consultation with all relevant stakeholders,[32] including privacy commissioners across all jurisdictions.[33]

21.25 The Public Interest Advocacy Centre expressed the view that, while there was a need to clarify when it is not reasonable and practicable to collect personal information directly from the individual, such guidance should be contained in the *Privacy Act*, the regulations or a binding code.[34]

21.26 Similarly, many stakeholders submitted that the principle itself ought to include a number of exceptions, including:

- for the collection of personal information for statistical and research purposes;[35]

- for the appropriate verification of an individual's circumstances from reliable third parties, including for the purposes of: facilitating health benefits and social services; providing support for disadvantaged customers; and preventing or lessening the instances of fraud;[36]

- where the party from whom the organisation or agency intends to collect the personal information of another individual has: the express or implied consent of that individual; actual or ostensible authority to act on behalf of the individual;

---

29 Ibid. The Office of the Victorian Privacy Commissioner noted that an individual may need to disclose information about their family circumstances when applying for financial assistance or welfare benefits: Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

30 Government of South Australia, *Submission PR 565*, 29 January 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

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

32 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007: The NHMRC submitted that it would be pleased to assist in the development of guidance on when it would not be reasonable and practicable to collect directly from the individual in the context of health care and human research: National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.

33 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

34 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. GE Money similarly expressed the view that 'to the greatest extent possible, the Act and the Regulations should stand alone as a clear compliance framework for organisations': GE Money Australia, *Submission PR 537*, 21 December 2007.

35 Australian Institute of Health and Welfare, *Submission PR 552*, 2 January 2008; Australian Bureau of Statistics, *Submission PR 383*, 6 December 2007.

36 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

or carer or parental responsibilities and duties with respect to the individual; and[37]

- to allow agencies to perform their law enforcement functions properly, and collect criminal intelligence, including through the receipt of anonymous and confidential tip-offs.[38]

21.27 Other stakeholders also expressed concerns that the principle should not limit an agency's intelligence, investigative and compliance functions; and emphasised, for example, the impracticability of collecting personal information from a suspect or witness only from that person.[39]

21.28 The Australian Taxation Office (ATO), however, opposed the proposal outright. It expressed 'very strong concerns' that it would prejudice its activities and impose upon it a resource-intensive administrative burden. The ATO stated that it did not want to be placed in a position of having to rebut a presumption that it should collect information directly from an individual.

> Collecting information from third parties is an essential part of the investigative and compliance activities of the Tax Office. The proposed principles would prejudice necessary activities such as:
>
> • verifying information through independent third parties
>
> • using third parties as a first source of information in particular where serious tax non-compliance is suspected, including criminal activity
>
> • lawfully gathering and matching information about larger numbers of individuals for data matching activities, and
>
> • collecting and using information in the many reports of transactions that the taxation law requires third parties to provide to the Tax Office.
>
> The Tax Office believes that adequate protection is already in place for taxpayers when third party information is used.[40]

21.29 Other stakeholders noted the 'operational challenges' and 'human resource costs' associated with implementing the proposal. [41] For example, the Department of Families, Housing, Community Services and Indigenous Affairs expressed concern

---

37 Australia Post, *Submission PR 445*, 10 December 2007.

38 Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008.

39 Confidential, *Submission PR 448*, 11 December 2007; Confidential, *Submission PR 488*, 19 December 2007.

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

41 Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008; Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

about the 'potential impost on individuals having to provide the same information to multiple agencies'.[42]

21.30 Finally, a number of tribunals submitted that it would not be reasonable and practicable for them, in carrying out their review processes, to collect personal information only from the individuals concerned.[43]

ALRC's view

21.31 Agencies and organisations should be required to collect personal information only from the individual to whom the information relates, where it is reasonable and practicable to do so. Such a requirement increases the likelihood that personal information collected will be accurate, relevant, complete and up-to-date. It also gives individuals an opportunity to participate in the collection process. As noted above, this requirement already applies to organisations.

21.32 The qualification that the requirement applies only 'where reasonable and practicable' is significant, particularly as it applies to agencies. There will be many situations where it will not be reasonable or practicable to collect personal information directly from the individual concerned. For example, the requirement is not intended to limit the coercive information-gathering powers of agencies, or the exercise of their intelligence, investigative and compliance functions. As noted above, the Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 acknowledged expressly that it will not be reasonable and practicable to collect personal information directly from an individual where direct collection would prejudice the purpose of collection, such as where a law enforcement body is investigating a breach of a criminal law.

21.33 Some stakeholders expressed the view that the principle itself should set out a number of circumstances when it would not be reasonable and practicable for the requirement to apply. It would be inconsistent with the adoption of high-level principles to introduce detailed and prescriptive rules concerning the application of this requirement.[44]

21.34 The OPC should develop and publish further guidance, in consultation with relevant stakeholders, to clarify when it would not be reasonable and practicable to collect personal information only from the individual concerned. While the OPC's current guidance addresses the general factors to be considered in assessing whether it is reasonable and practicable to collect personal information directly from an individual, the ALRC recommends that the further guidance address specific

---

42 Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 January 2008.

43 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 533*, 21 December 2007; Administrative Appeals Tribunal, *Submission PR 481*, 17 December 2007.

44 See Rec 18–1.

circumstances where direct collection may not be reasonable and practicable. In particular, taking into account the views expressed by stakeholders about the areas requiring clarification, the guidance should address collection:

- of personal information by agencies pursuant to the exercise of their coercive information-gathering powers or in accordance with their intelligence-gathering, investigatory and compliance functions;
- of statistical data;
- of personal information in circumstances in which it is necessary to verify an individual's personal information;
- of personal information in circumstances in which the collection process is likely to, or will, disclose the personal information of multiple individuals; and
- from children, persons with a decision-making incapacity and those authorised to provide personal information on behalf of the individual.

21.35 The ALRC acknowledges the concerns expressed by a number of tribunals that it would not be reasonable and practicable for them, in respect of their review processes, to collect information directly from the individuals concerned. This is one of a number of concerns expressed by tribunals concerning the application of privacy principles to them. These concerns have been addressed in the ALRC's recommendation to exempt partially tribunals from the operation of the *Privacy Act*.[45]

Recommendation 21–1 The model Unified Privacy Principles should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.

Recommendation 21–2 The Office of the Privacy Commissioner should develop and publish further guidance to clarify when it would not be reasonable and practicable to collect personal information about an individual only from the individual concerned. In particular, the guidance should address collection:

(a) of personal information by agencies pursuant to the exercise of their coercive information-gathering powers or in accordance with their intelligence-gathering, investigative, and compliance functions;

45 See Rec 35–1.

(b) of statistical data;

(c) of personal information in circumstances in which it is necessary to verify an individual's personal information;

(d) of personal information in circumstances in which the collection process is likely to, or will, disclose the personal information of multiple individuals; and

(e) from persons under the age of 18, persons with a decision-making incapacity and those authorised to provide personal information on behalf of the individual.

Unsolicited personal information

Background

21.36 Agencies and organisations sometimes receive unsolicited personal information. This occurs where personal information is received by an agency or organisation that has taken no active steps to collect that information. This is increasingly common in the digital age where information can be transmitted easily and quickly.

21.37 Sometimes unsolicited personal information received by an agency is particularly sensitive—for instance, in the area of community services, an agency may receive information relating to domestic violence or abuse. It has been noted that where such information remains on file, 'there is a danger that it will indirectly influence an agency official in their decisions about, or interactions with, the individual'.[46]

21.38 The IPPs, to some extent, make a distinction between the obligations imposed on an agency that solicits personal information and one that receives unsolicited personal information. IPPs 2 and 3 impose certain obligations on an agency only where it has solicited personal information. The obligations in IPP 1, however, which do not refer expressly to solicited information, have been said to apply where an agency receives unsolicited material—from sources such as a ministerial letter or a tip-off from an informer.[47]

21.39 NPP 1 does not distinguish between the obligations imposed on an organisation in respect of solicited and unsolicited information, although it does address separately personal information obtained directly from the individual concerned, and information

46 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.
47 See Explanatory Memorandum, Privacy Bill 1988 (Cth), [59].

collected from a third party.[48] This is relevant because unsolicited personal information tends to be received from third parties.

Submissions and consultations

21.40 In IP 31, the ALRC asked what obligations, if any, should apply to an agency or organisation when it receives unsolicited information that it intends to include in a record or a generally available publication.[49]

21.41 In response to IP 31, a number of stakeholders stated that, where an agency or organisation receives unsolicited personal information, this information should be covered by the privacy principles.[50] Some stakeholders suggested specific obligations that should apply in respect of unsolicited information:

- The 'accuracy of such information should be checked as soon as possible with the subject, where possible, unless the source is a publicly available source'.[51] The OPC submitted that this was particularly important where the information may be used to deny an individual 'access to essential services'.[52]

- The individual should be given the opportunity to give or withhold consent to his or her personal information being used in these circumstances.[53]

- Unsolicited information that is 'irrelevant to the functions' of the entity that receives it should be destroyed.[54]

21.42 Some stakeholders stated that no additional obligations should be imposed in respect of the collection of unsolicited information because the existing rules are sufficient.[55] Others suggested that it was not helpful to make a distinction between

---

48 See *Privacy Act 1988* (Cth) sch 3, NPPs 1.4, 1.5.

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

50 See, eg, 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; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

51 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. A number of other stakeholders expressed similar views: see, eg, Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007.

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

53 I Turnbull, *Submission PR 82*, 12 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

54 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007. A similar point was raised by Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

55 See, eg, Australian Federal Police, *Submission PR 186*, 9 February 2007; Confidential, *Submission PR 165*, 1 February 2007; Confidential, *Submission PR 143*, 24 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.

solicited and unsolicited information.[56] For example, the Centre for Law and Genetics argued that the distinction between solicited and unsolicited information derives from paper-based record keeping and 'should not be maintained in a modern computer-data driven environment'. It submitted that where an organisation or agency proposes to keep or use unsolicited information, it should be subject to the usual privacy principles.[57]

21.43 One stakeholder submitted that obligations only should be imposed on agencies or organisations in respect of unsolicited personal information which they retain.[58]

21.44 In DP 72, the ALRC proposed that the 'Collection' principle should provide that where an agency or organisation receives unsolicited personal information, it must either: (a) destroy the information immediately without using or disclosing it; or (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.[59]

21.45 There was some support for this proposal[60] and, more generally, for an approach providing for privacy protection regardless of whether personal information is obtained directly or indirectly from a third party.[61] The majority of stakeholders, however, expressed qualified support, raising three main areas of concern. The first was about the consequences of requiring unsolicited information to be destroyed immediately. Stakeholders stated that such an obligation was problematic because:

- an agency or organisation may need a deliberative period within which to consider whether to retain unsolicited personal information, and such deliberation ought to be a permitted use or disclosure;[62]

- it could make agencies and organisations 'hyper-vigilant' about destruction and could therefore lead to some information being destroyed in error; [63] and

---

56 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

57 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

58 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

59 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 18–2.

60 Anglicare Tasmania, *Submission PR 514,* 21 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; Australian Digital Alliance, *Submission PR 422,* 7 December 2007. The Australian Direct Marketing Association did not disagree with the proposal: Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007.

61 Australasian Compliance Institute, *Submission PR 419,* 7 December 2007.

62 See, eg, Confidential, *Submission PR 570,* 13 February 2008; Medicare Australia, *Submission PR 534,* 21 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500,* 20 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007.

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

- such a prescriptive approach would be financially and operationally onerous without delivering any clear extra privacy protection for individuals.[64]

21.46 The second area of concern was about nominating destruction as an option in certain circumstances. Stakeholders noted that destruction of personal information:

- was only an option where it did not breach the requirements of relevant records retention legislation;[65] and

- could impact negatively on accountability and audit requirements, leading, for example, to accusations of 'cover-ups' where a matter appears not to have been investigated.[66]

21.47 The third area of concern arose in relation to circumstances where stakeholders submitted that they would not be able to perform properly their functions if they were required either to destroy unsolicited information or comply with all the model UPPs in respect of that information. Particular concerns were expressed about complying with the 'Notification' principle, which imposes obligations on agencies and organisations to notify or otherwise ensure an individual is aware of certain matters concerning the collection of his or her personal information. This concern arose principally in relation to reliance by agencies on unsolicited personal information via anonymous and confidential tip-offs in order to investigate offences and non-compliant activity, as well as part of the general practice of collecting criminal intelligence.[67] Other contexts in which this concern arose included where:

- the Administrative Review Tribunal receives unsolicited information about third parties during its review processes;[68] and

- schools receive unsolicited information from other schools about the behaviour and needs of pupils who are transferring schools.[69]

---

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

65 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

66 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

67 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Australian Federal Police, *Submission PR 545*, 24 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

68 Administrative Appeals Tribunal, *Submission PR 481*, 17 December 2007.

69 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

21.48 Other stakeholders expressed qualified support for the proposal, on the basis that it was made clear that:

- 'using or disclosing' unsolicited personal information includes taking *any* action; and

- the option to destroy the information is exercised within a limited time, otherwise the obligations concerning data security would apply.[70]

21.49 A small number of stakeholders expressed outright opposition to the proposal on various grounds, including that it:

- is unnecessary or a matter more appropriately dealt with by OPC guidance, because organisations are currently subject to the privacy principles regardless of whether they receive personal information via solicited or unsolicited means;[71]

- will place unnecessary burdens on agencies to require them to meet the notification obligations in respect of unsolicited information;[72] and

- may be inappropriate for organisations to destroy immediately unsolicited personal information. For example, they may be required to retain the information for a period of time to consider its contents, check its accuracy or assess whether they have an obligation to act on the information received.[73]

21.50 A small number of stakeholders suggested that the meaning of 'unsolicited' should be clarified.[74] The Cyberspace Law and Policy Centre, and the Australian Privacy Foundation expressed the view that the *Privacy Act* or the Explanatory Memorandum to the amending legislation should make it clear that unsolicited personal information is included within the meaning of 'collect'.[75] The OPC noted that there are a number of ways in which personal information may be received without being solicited, for example via misdirected mail, promotional material, or third parties. It suggested that it publish guidance to clarify the meaning of 'unsolicited' in the context of the 'Collection' principle.[76]

---

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

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

72 Queensland Government, *Submission PR 490*, 19 December 2007.

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

74 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.

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

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

ALRC's view

21.51 Many agencies and organisations receive a large amount of unsolicited personal information. The fact that an agency or organisation has done nothing to cause personal information to be sent to it should not mean, however, that such information falls outside the protection of the privacy principles.

21.52 The risk that personal information will be used or disclosed in violation of a person's privacy only becomes significant where, on receiving unsolicited personal information, the agency or organisation retains it. If an agency or organisation is required, or decides, to retain unsolicited personal information then it should comply with all of the privacy principles in respect of that information, as if the agency or organisation had taken active steps to collect the information.

21.53 An agency or organisation may have no option but to retain personal information. For example, retention may be required because of the requirements of records retention legislation such as the *Archives Act 1983* (Cth) or it may otherwise be reasonable to retain the information in light of accountability, audit or evidentiary requirements.

21.54 Some stakeholders expressed concerns that they would not always be able to comply with the obligations imposed by the privacy principles in respect of certain unsolicited information. Compliance with the 'Notification' principle raised particular concerns. It is important to emphasise, however, that the requirement to comply with relevant privacy principles encompasses a consideration of any qualifications or exceptions to those principles. For example, the obligation to notify or otherwise ensure that an individual is aware of certain matters concerning the collection of his or her personal information is limited to taking such steps, if any, that are reasonable in the circumstances. In some circumstances it will be reasonable for an agency or organisation to take no steps to notify an individual about the collection of personal information. Such circumstances may include the receipt of unsolicited confidential 'tip-offs' relating to unlawful activity.[77]

21.55 A requirement to destroy immediately unsolicited personal information is impracticable, and an agency or organisation will require a deliberative period within which to consider whether it can lawfully collect the unsolicited information and whether it wishes to retain that information. If the collection is lawful and the agency or organisation decides to keep the information then, as stated above, the obligations that apply to the 'active' collection of personal information should apply. If the collection is unlawful or the agency or organisation does not wish to retain the information then the agency or organisation should destroy the information as soon as

77 The 'Notification' principle is discussed in Ch 23.

practicable without using or disclosing it—if it is lawful and reasonable to do so. A use or disclosure made for the purpose of determining whether the information needs to be retained should, however, be permissible. For example, an agency or organisation may need to use or disclose the information in order to receive advice about whether to retain or destroy it.

21.56 The above approach ensures that the spectrum of personal information that an agency or organisation may lawfully retain, use and disclose is not expanded merely because the entity has taken no steps to collect the information. The threshold requirement that an agency or organisation is only permitted to collect personal information that is 'necessary for one or more of its functions or activities' also should apply to the retention of unsolicited personal information.

21.57 The OPC should develop and publish guidance about the meaning of 'unsolicited' in the context of the 'Collection' principle. The ALRC notes the OPC's support for the development of such guidance.

Recommendation 21–3 The 'Collection' principle should provide that, where an agency or organisation receives unsolicited personal information, it must either:

(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 model Unified Privacy Principles that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

Recommendation 21–4 The Office of the Privacy Commissioner should develop and publish guidance about the meaning of 'unsolicited' in the context of the 'Collection' principle.

Other aspects of the 'Collection' principle

Location of notification requirements

21.58 As noted above, the collection principles in both the NPPs and IPPs provide that, in certain circumstances, agencies and organisations must ensure that an individual whose personal information has been, or is to be, collected, is aware of a number of matters. One way of ensuring awareness is through notification. A question arises whether the 'Collection' principle should set out notification requirements that apply at or around the time personal information is collected, or whether these

requirements should be set out in another principle that more explicitly relates to notification.

21.59 This issue is dealt with in Chapter 23, where the ALRC recommends that the notification requirements that are currently located in the collection principles in the IPPs and NPPs should be moved to a separate privacy principle called 'Notification'.[78]

Collection of sensitive information: location of provisions

21.60 Currently, the collection of sensitive information by organisations is covered in a separate privacy principle, NPP 10. The collection of sensitive information by agencies is not dealt with explicitly in the IPPs.

21.61 There is a question whether the 'Collection' principle also should deal with the collection of sensitive information, or whether the collection of sensitive information should be dealt with in a separate principle. This question is addressed in Chapter 22, where the ALRC recommends that the provisions that relate to the collection of sensitive information should be contained in the 'Collection' principle.[79]

Limitation on collection: reasonable purposes?

Background

21.62 As noted above, currently an organisation is prohibited from collecting personal information unless the information is necessary for one or more of its functions or activities.[80] An agency only may collect personal information if the:

- information is collected for a lawful purpose directly related to a function or activity of the agency; and
- collection of that information is necessary for, or directly related to, that purpose.[81]

21.63 The OPC's guidelines on collection of information by organisations provide that:

> The Commissioner interprets 'necessary' in a practical sense. If an organisation cannot in practice effectively pursue a legitimate function or activity without

78 See Rec 23–1.
79 See Rec 22–1. A summary of the 'Collection' principle, UPP 2, is set out at the end of this chapter. It includes the provisions relating to the collection of sensitive information. The collection of sensitive information, however, is discussed in Ch 22, and the collection of sensitive information for the purpose of research is discussed in Ch 65.
80 *Privacy Act 1988* (Cth) sch 3, NPP 1.1.
81 Ibid s 14, IPP 1.1.

> collecting personal information, then the Commissioner would ordinarily consider it necessary for that function or activity.[82]

21.64 The High Court of Australia has also noted that 'there is, in Australia, a long history of judicial and legislative use of the term "necessary", not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[83] A question arises whether agencies and organisations only should be able to collect personal information for purposes that a reasonable person would consider appropriate in the circumstances.

21.65 Some Canadian privacy law, for example, provides for an objective test in these circumstances. For instance, the federal legislation provides that an organisation may collect, use or disclose personal information 'only for purposes that a reasonable person would consider are appropriate in the circumstances'.[84] Similarly, Alberta's information privacy legislation states:

> Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.[85]

21.66 The Australian Privacy Foundation submitted to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry) that the NPPs should provide that collection be limited by such an objective test.[86] The OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) rejected the adoption of an objective test to ascertain whether collection of personal information is necessary for an organisation's functions or activities. It stated that, while it would enable an individual to challenge the collection of personal information, it would be difficult to implement in practice and 'it is not likely that the benefits of doing so would outweigh the costs'.[87]

Submissions and consultations

21.67 In DP 72, the ALRC proposed that the 'Collection' principle in the model UPPs should provide that an agency or organisation must not collect personal information

---

82 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 27.

83 *Mulholland v Australian Electoral Commission* (2004) 220 CLR 181, [39].

84 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 5(3). See also s 3.

85 *Personal Information Protection Act 2003* RS (Alberta) c.P–6.5 s 11(2). In IP 31, the ALRC sought views on whether a similar test should be introduced in the *Privacy Act*: See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.68], [11.127]. This issue, however, was not addressed by stakeholders, other than the OPC.

86 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.170]. See also Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.

87 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 91.

unless it reasonably believes the information is necessary for one or more of its functions or activities.[88]

21.68 Stakeholders' opinions on this proposal were divided. Some stakeholders supported the introduction of a 'reasonable belief' test.[89] A number of stakeholders however, expressed a preference for a more objective test, where what is reasonable is determined from the perspective of a reasonable person and not the agency or organisation.[90] For example, the Office of the Victorian Privacy Commissioner submitted:

> Agencies or organisations should only collect personal information that is necessary for their functions or activities, not information that an agency or organisation reasonably believes may be necessary for their functions or activities. The distinction is an important one: in the former case the test is an objective one which is determined by a regulator; in the latter case the test is a subjective one which is determined by the organisation collecting the information.[91]

21.69 The OPC expressed its support for the proposal, but submitted that the reasonableness of the *purpose* of collection also should be addressed.[92]

> Establishing that the purpose of collection is reasonable is more important than whether there is a reasonable necessity. If only the latter requirement applied, collections may be necessary, albeit for purposes that would seem unreasonable and beyond what individuals may expect is a reasonable function or activity of that organisation or agency …
>
> Accordingly, the Office reiterates the potential value of a collection principle requiring that an organisation may only collect personal information for purposes that are reasonable, where 'reasonable' means 'what a reasonable person would consider appropriate under the circumstances'.[93]

---

88 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 18–3.

89 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; 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 stated that it did not disagree with the proposal: Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007.

90 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007; I Graham, *Submission PR 427,* 9 December 2007. See also Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007, which expressed a preference for the test used in Canadian privacy law. The Public Interest Advocacy Centre submitted that 'a more objective and appropriate approach would be to focus on the information itself and to ask whether that information is reasonably necessary for one of more of the agency or organisation's functions or activities': Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007.

91 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

92 Other stakeholders expressed a similar view: Australian Privacy Foundation, *Submission PR 553,* 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007.

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

21.70 Some stakeholders submitted that the proposal should include requirements that:

- collection is proportional to the functions or activities of the agency or organisation;[94]
- there is a relationship between the perceived necessity of collection and the particular purpose of collection of the information in question;[95] and
- collection is for a lawful purpose.[96]

21.71 Other stakeholders opposed the proposal on varying grounds, namely that:

- it is unnecessary because the intent in the requirement in NPP.1 is sufficiently clear;[97]
- the test is too strict, and agencies should be able to continue to collect information because it will directly assist in achieving a lawful purpose without having to establish that a particular collection is necessary to achieve that purpose;[98] and
- the requirement for belief in the necessity of information is impracticable in certain contexts.[99]

ALRC's view

21.72 The ALRC acknowledges the concerns expressed by some stakeholders that the test proposed in DP 72 is not sufficiently objective. What is 'necessary' for the functions or activities of an agency or organisation should be determined objectively, rather than by the subjective belief of the agency or organisation.

21.73 An objective test is necessary to ensure appropriate privacy protection in circumstances where an agency or organisation claims that it is necessary to collect an individual's personal information for the legitimate purpose of providing a service to the individual, but the agency's or organisation's *real* purpose is an illegitimate one—

---

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

95 Ibid.

96 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; I Graham, *Submission PR 427*, 9 December 2007. Some stakeholders also submitted that this requirement should apply to the maximum extent practicable to information: obtained from observation or surveillance; extracted from other records; and generated within an organisation or agency as a result of a transaction: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

97 Confidential, *Submission PR 570*, 13 February 2008.

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

99 Confidential, *Submission PR 488*, 19 December 2007.

such as on-selling the data to a third party. In such situations, agencies and organisations should not be able to rely simply on their subjective views about the necessity of the collection, even where those views may have a reasonable basis. Rather, the test for necessity should be from the perspective of a reasonable person.

21.74 An objective test should encourage organisations and agencies to give careful consideration to whether the personal information they collect is genuinely necessary for their functions or activities.

21.75 The requirement in NPP 1 that an organisation must not collect personal information unless it is 'necessary for one or more of its functions or activities' implies an objective test—the collection has to be necessary, not necessary merely in the opinion of the organisation. Such an interpretation is also within the spirit of the privacy principles as a whole.

21.76 The requirement in NPP 1 should be applied to agencies as well as organisations. As discussed in Chapter 18, the NPPs should form the general template in drafting and structuring the UPPs. The wording of NPP 1 arguably is simpler than that of its equivalent provision, IPP 1.

21.77 It is unnecessary for the 'Collection' principle to provide expressly that the perspective of the reasonable person is to be applied in determining the necessity of the collection. It is also unnecessary to provide expressly that the purpose of collection is to be lawful and objectively reasonable. It is implied that the activities and functions pursuant to which agencies and organisations collect personal information must be lawful. It also is implied that collection pursuant to those functions must be lawful. The 'Collection' principle does not, and cannot, make unlawful collections lawful, such as where agencies collect information beyond the scope of their powers. In the case of sensitive information, the restrictions placed on collection assist in ensuring that the purposes of collection are reasonable. For example, it is reasonable to collect sensitive information because it is required by law or necessary for the establishment of a legal claim.[100]

21.78 The ALRC notes the ATO's concerns about the strictness of prohibiting collection of personal information unless it is necessary for an entity's functions or activities. This approach is consistent with IPP 1, however, which also includes a requirement of necessity. Further, such concerns may be assuaged somewhat by the fact that, historically, what is 'necessary' has been interpreted in a practical and liberal manner, as noted above.

---

100 Sensitive information is discussed in Ch 22.

Recommendation 21–5 The 'Collection' principle in the model Unified Privacy Principles should provide that an agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

Methods of collection

21.79 NPP 1 and IPPs 1–3 apply generally to the collection of personal information. They do not refer to particular methods of collection.

21.80 Privacy advocates submitted that the *Privacy Act*, or the Explanatory Memorandum to the amending legislation, should make it clear that the 'Collection' principle applies to specific methods of collection—namely to information that is: obtained by observation or surveillance; extracted from other records, such as books; and generated internally as a result of transactions.[101] Privacy advocates acknowledged that 'the practice of Privacy Commissioners seems to assume that observations [by surveillance] constitutes collection, and case law to the contrary is not known'.[102]

21.81 It is unnecessary to amend the Act to refer to specific methods of collection. The ALRC is not convinced that a mischief has been identified warranting such an amendment. It is clear that personal information may be collected by surveillance. The OPC's guidance on the obligation in NPP 1 for an organisation to collect personal information only by lawful and fair means and not in an unreasonably intrusive manner acknowledges the possibility that personal information may be collected by surveillance. The guidance notes that there will be some circumstances, for example, investigation of fraud or other unlawful activity, where covert collection of personal information by surveillance or other means would be fair.[103]

21.82 It is also clear that personal information may be collected from publicly available sources, such as books. Guidance issued by the OPC confirms this approach.[104]

Summary of 'Collection' principle

21.83 The second principle in the model UPPs should be called 'Collection'. It may be summarised as follows.

---

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

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

103 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 27.

104 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003). The OPC has noted that this Information Sheet has gained widespread support: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 262.

UPP 2. Collection

2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

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

(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.

2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented;

(b) the collection is required or authorised by or under law;

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;

(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual's consent;

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(f) the collection is necessary for research and all of the following conditions are met:

(i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable;

(ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;

(iii) 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*; and

(iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or

(g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Note: Agencies and organisations that collect personal information about an individual from an individual or from someone else must comply with UPP 3.

22. Sensitive Information

Contents

Introduction

22.1 This chapter discusses issues concerning the handling of sensitive information and, in particular, the collection of sensitive information. It focuses on three main issues. The first is whether the restrictions currently imposed on organisations by the National Privacy Principles (NPPs) concerning the collection of sensitive information also should be imposed on agencies. Secondly, it considers whether specific current exceptions to the general prohibition against the collection of sensitive information are in need of reform. Finally, it considers whether the *Privacy Act 1988* (Cth) should regulate aspects of the handling of sensitive information in addition to collection. This could include the use, disclosure, storage, access, retention and disposal of sensitive information.

Background

22.2 'Sensitive information' is a subset of 'personal information'. 'Sensitive information' is defined in s 6(1) of the *Privacy Act* to mean information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices; or
- criminal record.

22.3 'Sensitive information' also includes health information[1] and genetic information about an individual that is not otherwise health information.[2]

22.4 In general terms, there is a correlation between the categories of sensitive information provided for in the *Privacy Act* and the grounds of discrimination provided for under federal and state legislation.[3] Similarly, Australia's international law obligations are triggered by an asylum seeker who has a well-founded fear of persecution by reason of his or her 'race, religion, nationality, membership of a particular social group or political opinion'.[4] The fact that three of these grounds—race, religion and political opinion—are also categories of 'sensitive information' in s 6(1) of the *Privacy Act* reflects the inherent dangers that may arise where personal information of this nature is misused.

22.5 Sensitive information is given a higher level of protection under the NPPs; in particular, in relation to its collection. The Information Privacy Principles (IPPs), in contrast, do not provide for additional protection in respect of any aspect of the handling of sensitive information by agencies. The current coverage of the NPPs and IPPs is discussed below.

---

1 *Privacy Act 1988* (Cth) s 6(1). The definition of 'health information' is discussed in Ch 62.

2 The definitions of 'personal information' and 'sensitive information' are discussed in more detail in Ch 6, as are the ALRC's recommendations concerning their amendment.

3 Compare *Privacy Act 1988* (Cth) s 6(1) with, eg, *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Disability Discrimination Act 1992* (Cth).

4 See *Migration Act 1958* (Cth) s 36, incorporating the *Convention relating to the Status of Refugees*, 28 July 1951, [1954] ATS 5, (entered into force generally on 22 April 1954).

22.6 There is international precedent for providing additional privacy protections in respect of sensitive information. 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) recognises 'special categories of data', which are defined as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'.[5] Article 8 prohibits the processing of this kind of information without consent, except in specified circumstances. It also allows member states to prohibit the processing of such information, even with the consent of the individual concerned.

22.7 A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up under art 29 of the EU Directive, highlighted the importance of providing additional protection to sensitive information, by stating that

> where 'sensitive' categories of data are involved … additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.[6]

22.8 The *Data Protection Act 1998* (UK), for example, prohibits the processing of sensitive information unless one of ten specified conditions apply.[7]

Collection of sensitive information

Current coverage by IPPs and NPPs

22.9 The IPPs do not regulate the collection of sensitive information separately from other forms of personal information. In contrast, NPP 10 regulates separately and specifically the collection of sensitive information. It prohibits the collection of such information, except in certain identified circumstances. NPP 10.1 provides that sensitive information can be collected only if the:

- individual has consented;
- collection is required by law;

---

5 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.

6 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. See also *Personal Information Protection and Electronic Documents Act 2000 SC 2000, c 5 (Canada)* sch 1, cl 4.3.6, which provides that an organisation should generally seek express, as opposed to implied, consent when the information is likely to be considered sensitive.

7 See *The Data Protection Act 1998 (UK)* sch 1, Principle 1; sch 3.

- collection is necessary to prevent or lessen a serious and imminent threat to the life or health of an individual and the individual is physically or legally incapable of giving or communicating consent to the collection; or

- collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

22.10 In addition, NPP 10.1 allows sensitive information to be collected in the course of the activities of a non-profit organisation.[8] This is permitted where: the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and at, or before, the time of collection the organisation undertakes to the individual that it will not disclose the information without the individual's consent.

22.11 NPPs 10.2, 10.3 and 10.4 regulate the collection of health information by organisations. Health information is a category of sensitive information. Issues concerning the collection of health information are discussed in Chapter 63.

Expansion of sensitive information provisions to agencies?

Background

22.12 The fact that the IPPs do not contain a principle dealing specifically with the collection of sensitive information is consistent with the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines), which also do not contain such a principle. Indeed, the Explanatory Memorandum to the OECD Guidelines states that 'it is probably not possible to identify a set of data which are universally regarded as being sensitive'.[9] In contrast, as noted above, the EU Directive imposes additional restrictions on the processing of sensitive information, which includes the collection of such information by agencies and public authorities.[10]

22.13 Should agencies also be subject to restrictions in collecting sensitive information? There is precedent for such a position in Australian jurisdictions as Victorian, Tasmanian and Northern Territory privacy legislation imposes restrictions on the collection of sensitive information by agencies.[11]

---

8 Non-profit organisation here means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims. See *Privacy Act 1988* (Cth) sch 3, NPP 10.5.

9 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19(a)].

10 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 2.

11 *Personal Information Protection Act 2004* (Tas) sch 1, IPP 10(1); *Information Act 2002* (NT) sch, IPP 10.1; *Information Privacy Act 2000* (Vic) sch 1, IPP 10.1.

Submissions and consultations

22.14 In response to Issues Paper 31, *Review of Privacy* (IP 31), a number of stakeholders submitted that agencies, like organisations, also should be subject to a 'sensitive information' privacy principle.[12]

22.15 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that agencies, as well as organisations, should be subject to requirements relating to the collection of sensitive information, as defined in the *Privacy Act*, and that these requirements should be located in the 'Collection' principle.[13] There was general support for this approach.[14] Reasons given for supporting the extension of the requirements to agencies include that:

- Individual's sensitive information requires consistency of protection regardless of whether that information is handled by a public or private sector entity;[15]
- risks associated with subsequent misuse of this information are no less serious where the information is collected by an agency;[16] and
- such an approach is consistent with that taken in Victoria, Tasmania and the Northern Territory.[17]

22.16 Stakeholders supported locating the collection of sensitive information provisions within the 'Collection' principle on the basis that:

- a separate privacy principle for sensitive information would be 'unnecessarily complicated';[18] and

---

12 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 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.

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

14 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 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 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 (ADMA) 'did not disagree' with this approach: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

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

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

17 Ibid. See also Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

- it would assist relevant entities 'to navigate the *Privacy Act* and to understand their specific obligations'.[19]

22.17 Two stakeholders expressed support 'in principle' only.[20] The Australian Federal Police expressed support on the basis that there would be an appropriate exemption to enable law enforcement agencies to perform their functions.[21] The Australian Privacy Foundation expressed reservations about certain exceptions to the general prohibition against the collection of sensitive information.[22]

22.18 The Department of Agriculture, Fisheries and Forestry noted that this approach represented a 'fundamental new direction for the public sector'.[23] Medicare Australia, expressed some concerns about the ramifications of the proposal.

> Given that agencies have not up to now been required to categorise relevant personal information as 'sensitive', careful consideration would be required as it may have consequences for the administration and payment of claims for government health benefits.[24]

ALRC's view

22.19 There are strong policy reasons to require agencies, and not just organisations, to be subject to restrictions relating to the collection of sensitive information. An individual's sensitive information should not be subject to lesser protections concerning its initial collection merely because it is collected by an agency rather than an organisation.

22.20 The finite list of categories of personal information that comprise sensitive information have been treated differently from other forms of personal information because, if misused, the information can be particularly damaging to the individual concerned or those associated with the individual. As explained in Chapter 6, information relating to race or ethnic origin, political or religious beliefs, trade union membership and sexual orientation, for example, is highly personal and may provide the basis for unjustified discrimination and other forms of mistreatment.

22.21 The risks associated with sensitive information being subsequently misused are sufficiently serious to justify imposing an obligation on agencies to abide by restrictions on the collection of sensitive information. Such restrictions however,

---

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

20 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Federal Police, *Submission PR 545*, 24 December 2007.

21 Australian Federal Police, *Submission PR 545*, 24 December 2007.

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

23 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

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

should allow for the collection of sensitive information by agencies for legitimate reasons.[25]

22.22 The provisions dealing with the collection of all personal information, including sensitive information, should be located in a single privacy principle called 'Collection' in the model Unified Privacy Principles (UPPs). Locating the provisions within a single principle emphasises the obligations to be imposed on agencies and organisations at the collection stage of the information cycle.

22.23 It is illogical to deal with the collection of sensitive information in a separate privacy principle, particularly as the existence of a separate principle can convey the incorrect impression that there is a completely separate regime applicable to sensitive information at all stages of the information cycle.[26] Further, the approach recommended by the ALRC is consistent with that taken in NPP 2, which includes a consideration of the use and disclosure of all personal information, including sensitive information, where relevant.[27]

Recommendation 22–1 The model Unified Privacy Principles should set out the requirements of agencies and organisations in relation to the collection of personal information that is defined as 'sensitive information' for the purposes of the *Privacy Act*. These requirements should be located in the 'Collection' principle.

Required or authorised by or under law

Background

22.24 NPP 10.1(b) contains an exception to the prohibition against the collection of personal information where it is required by law. There is no exception where a collection is authorised, but not required, by or under law.[28] As agencies are currently not subject to any separate restrictions concerning the collection of sensitive information, they are able to collect such information where it is authorised by law, provided that the collection complies with the IPPs regulating the collection of personal information.

25 The ALRC's view on collection of sensitive information required or authorised by or under law is discussed below.

26 The ALRC's view on regulating sensitive information separately to other forms of personal information in other aspects of the information cycle is discussed below.

27 This approach has been taken by the ALRC also in UPP 5 dealing with use and disclosure.

28 The phrases 'required by or under law' and 'authorised by or under law' are discussed in detail in Ch 16.

22.25 An issue arises as to whether there should be an exception to the general prohibition against the collection of sensitive information where the particular collection is authorised, or specifically authorised, by or under law.[29] The issue is pertinent particularly in light of the ALRC's recommendation to subject agencies to restrictions on the collection of sensitive information.

Submissions and consultations

22.26 In response to IP 31, the Australian Government Department of Health and Ageing (DOHA) submitted that the absence of an exception to the general prohibition against the collection of sensitive information where a collection is authorised by law would 'impose significant limitations on agencies', for example, by preventing them from collecting sensitive information from third parties unless specifically required to do so. DOHA submitted that there should be an exception to the prohibition on collecting sensitive information where the collection is required *or authorised* by law.[30]

22.27 In DP 72, the ALRC proposed that the sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or specifically authorised by or under law.[31]

22.28 Stakeholders views on this proposal were divided. There was some support for this approach.[32] For example, the Public Interest Advocacy Centre (PIAC) acknowledged that agencies and organisations still must be able to collect sensitive information for legitimate purposes, and that to allow only collections 'required by law' was too narrow.[33] The Office of the Privacy Commissioner (OPC) supported the condition of 'specific authorisation' being added, stating that it was appropriate particularly in the context of sensitive information.[34]

22.29 Some stakeholders, however, expressed strong concerns about the proposed condition requiring collection to be 'specifically' authorised, particularly as it applied to agencies.[35] They submitted that such a requirement would:

---

29 Arguments supporting the inclusion of a requirement that an act or practice be 'specifically authorised' are set out in Ch 16.

30 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007. The Department noted that such an amendment would render the provision currently in NPP 10.2 redundant.

31 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 19–2.

32 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; Optus, *Submission PR 532*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

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

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

35 Australian Federal Police, *Submission PR 545*, 24 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Victoria Police, *Submission PR 523*, 21 December 2007; Australian Communications and Media Authority, *Submission*

- create 'rigidity' not in keeping with the intended flexibility of the high level principles;[36]

- have potentially far reaching implications and may affect the capacity of agencies to fulfil their statutory functions and powers;[37]

- be difficult to establish, because express specific authorisation to collect categories of sensitive information—such as criminal records or details of membership of trade or professional associations—will not usually be provided for in legislation, although it may be necessarily implied that in certain circumstances agencies have this authority;[38] and

- require a careful review of current legislation to ensure that sensitive information required by agencies to administer properly government programs is specifically mentioned.[39]

22.30 The Office of the Victorian Privacy Commissioner (OVPC) opposed the proposal on a different basis. In its view, the proposal was not stringent enough. The OVPC submitted that the requirement to collect sensitive information must be mandatory, and not simply permissive or discretionary.[40]

ALRC's view

22.31 An exception which permits agencies and organisations to collect sensitive information where the collection is required by law is too narrow. The 'Collection' principle must contain an exception which allows for the legitimate collection of sensitive information authorised by law. Agencies, in particular, may need such information to fulfil their statutory functions, including those relating to law enforcement and the administration of government programs.

PR 522, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; Confidential, *Submission PR 448*, 11 December 2007.

36 Queensland Government, *Submission PR 490*, 19 December 2007.

37 Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007. Victoria Police recommended that law enforcement functions be included in the exception: Victoria Police, *Submission PR 523*, 21 December 2007.

38 Australian Federal Police, *Submission PR 545*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Victoria Police, *Submission PR 523*, 21 December 2007; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Confidential, *Submission PR 448*, 11 December 2007.

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

40 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

22.32 The ALRC acknowledges the concerns expressed by stakeholders that 'specific' authorisation to collect sensitive information is rarely provided for in legislation. Many agencies possess generally worded coercive information-gathering powers, which do not refer specifically to sensitive information. Imposing a 'specific authorisation' requirement would likely necessitate a review of current legislation to ensure that, where needed, the collection of sensitive information is specifically authorised. An exception which permits the collection of sensitive information where it is specifically authorised by or under law, therefore, is too restrictive, particularly in its application to agencies. The relevant exception to the prohibition against the collection of sensitive information should permit collection where it is required or authorised by or under law.

22.33 The ALRC considered an alternative option for reform, in light of the fact that most of the concerns expressed about the 'specific authorisation' requirement relate to its application to agencies. This alternative is to have an exception allowing for the collection of sensitive information by: agencies where it is required or authorised by or under law; and organisations where it is required or specifically authorised by or under law.

22.34 On balance, it would be simpler to have the same exception apply to both agencies and organisations to avoid the types of complications that currently arise due to the existence of a dual set of principles.[41] It should be emphasised that, under the recommended exception, agencies and organisations will still need to identify the law that requires or authorises their collection of sensitive information.

Recommendation 22–2 The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or authorised by or under law.

Emergency situations

Background

22.35 A question arises whether agencies and organisations should be able to collect sensitive information in emergency situations where an individual is unable to give consent. If so, how should such an exception to the general prohibition against the collection of sensitive information be framed?

22.36 Part VIA of the *Privacy Act*, which commenced operation on 7 December 2006, displaces some of the requirements in the IPPs and NPPs.[42] It provides a separate regime for the collection, use and disclosure of personal information where there is a

41 Such complications are discussed in Ch 18.

42 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).

connection to an emergency or disaster that has been the subject of a written declaration by the Prime Minister or a minister. The Part VIA regime is considered in more detail in Chapter 44.

22.37 The collection of sensitive information in emergencies not the subject of a declaration by the Prime Minister or minister, may be covered by the exception in NPP 10, which allows for the collection of sensitive information where it is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, and the individual whom the information concerns is incapable of giving consent.[43] The question arises whether this is an appropriately framed exception.

22.38 The principles covering use and disclosure of information by agencies and organisations similarly require that there be a 'serious and imminent' threat to the life or health of an individual.[44] Concern has been expressed, however, that the *Privacy Act* does not respond adequately to the need to share personal information in emergency situations. In the context of the use and disclosure principles, the requirement that there be a 'serious *and* imminent' threat to the life or health of an individual poses difficulties in practice because often it may only be possible to establish a serious *or* imminent threat. Particularly in the case of disaster recovery, the threat may be serious but no longer 'imminent'.[45]

22.39 By way of comparison, German privacy law, for example, specifically allows for the collection by public bodies of 'special categories of personal data' where: it is 'urgently needed to protect an important public interest'; 'it is urgently necessary in order to avert serious prejudice to the public interest or to safeguard important public interest concerns'; or 'it is necessary on compelling grounds relating to … obligations of the Federal Government in the area of crisis management or … for humanitarian measures'.[46]

Submissions and consultations

22.40 In DP 72, the ALRC proposed broadening the exception relating to emergency situations not the subject of a ministerial declaration under the Act, by permitting the collection of sensitive information by an agency or organisation where: the collection is necessary to lessen or prevent a serious threat to the life or health of any individual; and the individual whom the information concerns is incapable of giving consent.[47]

---

43 *Privacy Act 1988* (Cth) sch 3, NPP 10.1(c).

44 Ibid s 14, IPP 11; sch 3, NPP 2(e). The use and disclosure exception in NPP 2 applies also where there is a serious and imminent threat to the safety of an individual.

45 Use and disclosure of personal information in emergency situations is discussed in Ch 25.

46 *Federal Data Protection Act 1990* (Germany) s 13.

47 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 19–3.

22.41 The proposed removal of the requirement that a threat be 'imminent' received support from a range of stakeholders, including state privacy commissioners, organisations, and some public sector bodies.[48] For example, the OVPC stated that:

> The current requirement under NPP 10.1(c) and under the Victorian IPP 10.1(c) that a threat be both serious and 'imminent' may currently be too stringent to be effective. In my experience the requirement of imminence has led to uncertainty and confusion on the part of agencies.[49]

22.42 The South Australian Government supported the removal of the requirement that the threat be 'imminent', but suggested that the term 'imminent' be replaced with another term that suggests likelihood without implying urgency, such as 'probable' or 'likely'. It submitted that this would be 'consistent with a risk management approach, which generally assesses likelihood as well as consequence'.[50]

22.43 A small number of stakeholders, however, opposed the removal of the requirement that the threat be imminent, principally on the basis that it would lower privacy protections for individuals.[51] For example, the OPC expressed the view that an individual's privacy rights should not be undermined unnecessarily by virtue of his or her inability to give consent. It submitted that, if the requirement that the threat be 'imminent' is removed, then in cases where an individual is incapable of giving consent to a collection, agencies and organisations should be required to obtain consent from the individual's authorised representative, where it is reasonably practicable to do so.[52]

22.44 Similarly, PIAC expressed concern that:

> If the exception can be triggered simply when a threat is 'serious' it could be used to justify bulk collection of sensitive information without consent on the basis that the information may be useful at some time in the future to prevent serious harm (for example, collection of health information in respect of people with mental illness, where there may be a potential for serious threat to health, but no imminence, because the illness may be episodic, or controlled by medication).[53]

---

48 Confidential, *Submission PR 570,* 13 February 2008; 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; Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007; Privacy NSW, *Submission PR 468,* 14 December 2007; Tasmanian Government Department of Health and Human Services, *Submission PR 436,* 10 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.

49 Office of the Victorian Privacy Commissioner, *Submission PR 493,* 19 December 2007.

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

51 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.

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

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

22.45 Other aspects of the proposal received qualified support. Two stakeholders submitted that if there is a serious threat to the life or health of an individual, then the exception should apply regardless of whether an individual is capable of giving, or gives, consent to the collection.[54] One stakeholder expressed the view that the exception should be extended to allow collections of sensitive information where it is necessary to lessen or prevent a serious threat to public health or public safety.[55]

22.46 PIAC also submitted that there was a need to clarify whether 'incapable of giving consent' referred to physical or legal incapacity.[56]

ALRC's view

22.47 An agency or organisation should be permitted to collect sensitive information where such a collection is necessary to prevent or lessen a serious threat to the life or health of any individual, and the individual to whom the information concerns is incapable of giving consent. The provision relating to this exception should clarify that 'incapable of giving consent' extends to legal and physical incapacity to give or communicate consent, consistent with the approach in NPP 10.1(c).

22.48 As discussed in Chapter 25, the current requirement that a threat must be both serious *and* imminent is too difficult to satisfy. It can lead to personal information not being used or disclosed in circumstances where there are compelling reasons justifying its use or disclosure.[57] The relevant exception to the prohibition on the collection of sensitive information should be relaxed so that it is triggered where a threat is serious, but not necessarily imminent. This would allow an agency or organisation to take preventative action to stop a threat from developing into a crisis. This formulation strikes an appropriate balance between respecting the privacy rights of an individual and the public interest in averting threats to life and health.

22.49 The requirement that a threat be serious implies considerations of both consequence and likelihood.[58] It is not necessary to replace 'imminent' with another word suggesting likelihood, such as 'probable' or 'likely', as proposed by one stakeholder. If it is improbable that a threat will eventuate, then the threat cannot be considered serious.

22.50 Further, it is not necessary to extend the ambit of the exception to apply to the collection of sensitive information where it is necessary to lessen or prevent a serious threat to public health or public safety. Other exceptions to the prohibition on the

---

54 Confidential, *Submission PR 570*, 13 February 2008; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007.
55 Confidential, *Submission PR 570*, 13 February 2008.
56 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
57 See, in particular, Rec 25–3 and accompanying text.
58 This view is discussed further in Ch 25.

collection of sensitive information will address these concerns. Of particular application in this context is the exception which permits a collection required or authorised by or under law.[59] For example, state and territory public health legislation requires health service providers to collect and record certain information about health consumers with 'notifiable diseases', such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[60] In other cases, it may be possible for agencies and organisations to rely on the exception permitting collection where it is necessary to lessen or prevent a serious threat to the life or health of *any* individual, where that individual is incapable of consenting.

Recommendation 22–3 The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is legally or physically incapable of giving or communicating consent.

Other situations not involving a serious threat to life or health

Background

22.51 Concerns have been raised about the provision of services to vulnerable persons who are unable to provide informed consent in circumstances which may not necessarily involve a serious threat to life or health.

22.52 The Community Services Ministers' Advisory Council (CSMAC) expressed such a concern in the context of providing services to vulnerable persons, where those services are reliant on the collection of sensitive information. For example, those running accommodation services for homeless individuals will sometimes need access to information about the health of the individual before providing accommodation to that individual.[61]

22.53 The CSMAC queried whether a mere decline in health, or the dangers associated with 'sleeping rough', would be considered a 'serious threat to life or health', or whether a crisis event is required to trigger the exception. It noted that many err on the side of caution, thus affecting the accessibility of services for vulnerable individuals.[62] It stated that:

> A person may have impaired competence (either short or long term) to provide informed consent and there is no alternative consent provider, such as a legal guardian or family member. This is a frequent dilemma for homeless services, where the

59 See Rec 22–2.
60 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.
61 Community Services Ministers' Advisory Council, *Submission PR 47*, 28 July 2006.
62 Ibid.

> capacity to provide informed consent may be limited by factors such as the use of substances or mental health problems. In such circumstances, there is a dilemma about how to treat consent: a person might provide consent which is of dubious validity, or alternatively, may refuse consent but with a limited understanding of either the consent or the implications of their refusal, which may affect their treatment or access to services that they have requested.[63]

Submissions and consultations

22.54 In DP 72, the ALRC asked whether the collection of sensitive information should be permitted where all of the following conditions are met:

> (a) the individual is incapable of giving consent;
>
> (b) the collection is necessary to provide an essential service for the benefit of the individual; and
>
> (c) the collection would be reasonable in all the circumstances.[64]

22.55 Stakeholders' views on this issue were divided. Some stakeholders were supportive of the above approach, particularly in its application to the collection of health information.[65] For example, the National Health and Medical Research Council, expressed the view that such an approach

> will assist in the efficient delivery of health and personal care in circumstances where a paid carer is assisting a person who is incapable of giving consent to the carer collecting the person's health information (for example, when a personal carer collects pharmaceuticals on behalf of a person with dementia).[66]

22.56 Avant Mutual Group Ltd expressed qualified support on the assumption that:

- the incapable individual concerned does not have an appropriate person, such as a guardian or partner, to give consent on his or her behalf; and
- a medical practitioner is of the view that the withholding of treatment will compromise the individual's health.[67]

---

63 Ibid.

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

65 Government of South Australia, *Submission PR 565*, 29 January 2008; 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 was not opposed to inclusion of such an exception, provided the *Privacy Act* defined 'essential service' and the OPC issued binding rules relating to capacity to consent: Privacy NSW, *Submission PR 468*, 14 December 2007. Another stakeholder expressed the view that the exception should apply also to private health insurance and not just an 'essential service': Confidential, *Submission PR 519*, 21 December 2007.

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

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

22.57 A number of stakeholders, however, opposed such an exception to the collection of sensitive information.[68] Reasons for opposing the exception included that:

- there are inherent difficulties in defining 'essential services', particularly beyond what is covered by health information provisions—for example, it is unclear that financial services or welfare in general are properly described as 'essential', despite being potentially beneficial to an individual;[69]
- the question of what 'is reasonable in the circumstances' is unclear in its scope and application;[70]
- given its reliance on relatively vague terms, it may lead to regulatory complexity and uncertainty, as it may be difficult for the OPC to apply consistently;[71]
- it has the potential to be abused, because it appears to allow agencies and organisations to bypass seeking consent from an authorised representative of the incapable individual;[72]
- it is paternalistic and overlooks the fact that 'the consequences of collection in well-meaning circumstances may not necessarily be perceived by affected individuals as being beneficial';[73]
- it is unnecessary;[74] and
- while conceived with homeless persons in mind, it could have unintended or undesirable consequences.[75]

---

68 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.

69 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. The Office of the Victorian Privacy Commissioner expressed the view that if the provision is 'intended to apply to situations that deal only with "health information", perhaps it is better dealt with in that context': Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. Another stakeholder stated that it would be necessary or desirable to provide guidance about the types of essential services contemplated by the provision: Confidential, *Submission PR 570*, 13 February 2008.

70 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. The Office of the Victorian Privacy Commissioner expressed the view that 'great care needs to be taken to prevent "reasonable in all the circumstances" being broadly interpreted': Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

72 Ibid. See also Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. Another stakeholder expressed a similar view that it could lead agencies and organisations to 'avoid extra hurdles in their work': Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

74 Ibid.

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

22.58 The OPC suggested that service providers for homeless people consider applying for a Public Interest Determination (PID) to address the collection of sensitive information from persons lacking the capacity to give consent. The OPC submitted that a PID process is 'likely to permit more careful and deliberate consideration of the specific issue' than can be undertaken in the ALRC's wide ranging Inquiry. Further, it stated that:

> Unlike an amendment to the principles, a PID, if made, could also be drafted more precisely to ensure that its scope is more certain than a generally applicable exception to a collection principle. Such precision allows for regulation to be created that is narrow and focused on addressing the specific matter at hand.[76]

ALRC's view

22.59 The ALRC acknowledges the wide array of concerns expressed by stakeholders about the creation of an exception permitting the collection of sensitive information in order to provide essential services to individuals incapable of giving consent. The difficulties associated with the creation and implementation of such an exception significantly outweigh any potential benefit which it may confer on some vulnerable individuals. In particular, the ALRC agrees that defining 'essential service' is problematic, and that the adoption of such an exception may have unintended and undesirable consequences.

22.60 There is merit in the OPC's suggestion that PIDs in this area would provide for greater specificity and certainty in addressing the needs of particular vulnerable persons without risking the potential abuse of those persons' privacy. If it transpired that any PIDs granted—for example, to service providers for homeless people—were ineffective in balancing the welfare and privacy of vulnerable individuals, it would then be appropriate for further consideration to be given to the merits of implementing a legislative solution.

Research

22.61 In some state and territory privacy legislation, there is a research-related exception to the prohibition on collection of sensitive information by agencies, and this is broader than that provided for in NPP 10. For example, in Victoria and the Northern Territory, public sector bodies can collect sensitive information—not just health information—if:

- the collection is necessary for research, the compilation or analysis of statistics relevant to government funded targeted welfare or educational services, or

76 Ibid.

relates to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services;[77]

- there is no other reasonably practicable alternative to collecting the information for that purpose; and

- it is impracticable for the organisation to seek the individual's consent to the collection.[78]

22.62 This raises the question of whether the model UPPs should permit the collection of sensitive information for research in areas other than health and medical research. This question is addressed separately in Chapter 65. In accordance with the recommendations made in that chapter, the 'Collection' principle contains an exception addressing collection of sensitive information necessary for research, where certain conditions are met.[79]

Other exceptions

Background

22.63 Other exceptions to the prohibition against the collection of sensitive information, which are currently included in NPP 10.1, are:

- where the individual has consented;[80]

- if the information is collected in the course of the activities of a non-profit organisation where specified conditions are met;[81] and

- where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

22.64 The last-mentioned exception is worded in broader terms in the *Data Protection Act 1998* (UK). That Act provides that one of the conditions upon which sensitive information can be processed is where it is:

- necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or for obtaining legal advice; or

- otherwise necessary for the purposes of establishing, exercising or defending legal rights.[82]

---

77 See also *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(c).
78 *Information Privacy Act 2000* (Vic) sch 1, IPP 10.2; *Information Act 2002* (NT) sch, IPP 10.2.
79 The 'Collection' principle, UPP 2, is set out at the end of Ch 21.
80 Consent is discussed in Ch 19.
81 The definition of a 'non-profit organisation' is defined in NPP 10. 5 and set out above.
82 *Data Protection Act 1998* (UK) sch 3, cl 6.

Submissions and consultations

22.65 In DP 72, the ALRC included the above mentioned exceptions in the proposed 'Collection' principle. A small number of stakeholders submitted that these exceptions need to be amended. In particular, privacy advocates submitted that:

- express or explicit consent should be required for the collection of sensitive information;[83] and
- the exception relating to non-profit organisations should be redrafted.[84]

22.66 The Cyberspace Law and Policy Centre, for example, stated:

> We suggest a preferable alternative that refers directly to the definition of sensitive information in the Act, and adds the caveat that the activities must be lawful, to avoid the exception covering organisations' unlawful discrimination, race hate etc[85]

22.67 Specifically, privacy advocates suggested that the exception should be redrafted to allow the collection of sensitive information 'if the information is collected in the course of the lawful activities of a non-profit organisation that has aims relating to sensitive information (as defined in the Act)' where the existing conditions specified in NPP 10.2(d) are met.[86]

22.68 In addition, Avant Mutual Group Ltd (Avant) submitted that the exception relating to legal and equitable claims is too narrow, because it implies that it applies only to civil proceedings. Avant submitted that the exception should be broadened to

> take into consideration that legal advice of a general nature may be sought and legal services provided in anticipation of and/or for actual proceedings including a civil claim before a Court and responding to a professional disciplinary complaint or action or investigation before a Tribunal or Statutory Authority.[87]

---

83 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008. Two other stakeholders emphasised that there needs to be informed consent prior to the collection of sensitive information: Liberty Victoria—Victorian Council for Civil Liberties, *Submission PR 540*, 21 December 2007; Smartnet, *Submission PR 457*, 11 December 2007.

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

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

ALRC's view

Consent exception

22.69 While there are likely to be situations where it would be appropriate for express consent to be obtained before collecting sensitive information, it would be impracticable and overly prescriptive to require express consent for each collection. This is so particularly in the context of collecting health information. The OPC's *Guidelines on Privacy in the Private Health Sector*[88] note that there are situations where health service providers reasonably may rely on implied consent from individuals to handle health information in particular ways.[89] It should be emphasised that implied consent must still be voluntary, informed, and obtained from a person with capacity to consent.[90]

22.70 It is undesirable, therefore, to amend the consent exception to require express consent for the collection of sensitive information. Guidance from the OPC provides a more flexible mechanism for dealing with this issue. In Chapter 19, the ALRC recommends that the OPC should develop and publish guidance on consent which addresses express and implied consent as it applies in various contexts. The OPC's guidance should address the practice of bundled consent as it applies to the collection of sensitive information.

Exception relating to non-profit organisations

22.71 The concerns about the drafting of the exception relating to non-profit organisations will best be addressed by the Office of Parliamentary Counsel. That Office will be responsible for drafting amendments to the *Privacy Act*, including the UPPs, if the ALRC's recommendations are implemented by the Australian Government.

22.72 The definition of 'non-profit organisation' should be situated in Pt II of the *Privacy Act*, which deals with interpretation of terms, rather than in the 'Collection' principle.[91] It is logical to locate this definition with the other definitions in the Act. It also makes for simpler drafting of the exception relating to non-profit organisations within the 'Collection' principle.

Exception relating to legal and equitable claims

22.73 The ALRC is not convinced that there is a need to broaden the exception relating to the establishment, exercise or defence of legal and equitable claims. The ALRC did not receive sufficient feedback from stakeholders to enable it to assess properly the merits and consequences of broadening the exception. The ALRC does

---

88 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001).
89 This is discussed further in Ch 19.
90 The elements of consent are discussed in Ch 19.
91 The definition of 'non-profit organisation' currently appears in NPP 10.5.

not recommend an amendment to this exception. It appears in its current form as an exception to the 'Collection' principle in the model UPPs.

22.74 It is important to note, however, that the 'required or authorised by or under law' exception[92] may permit the collection of sensitive information pursuant to orders made by courts and tribunals.[93] This is relevant because such orders will frequently be made in the course of proceedings in respect of which a person is establishing, exercising or defending a legal or equitable claim. The exception may provide additional scope for permitting the collection of sensitive information in such circumstances.

Exception relating to alternative dispute resolution

22.75 For reasons discussed in detail in Chapter 44, the ALRC also is of the view that the collection of sensitive information should be permitted where it is necessary for the purpose of a confidential alternative dispute resolution process.

Regulation of other aspects of handling sensitive information

Background

22.76 As noted above, the IPPs do not impose special restrictions on the collection of sensitive information; nor do they distinguish between the treatment of sensitive information and non-sensitive personal information at other stages of the information cycle such as use, disclosure, access and disposal. Guidelines issued by the OPC acknowledge expressly that where sensitive information is concerned, 'more care to protect individuals' privacy may be appropriate than is required by the letter of the IPPs'.[94]

22.77 In addition to imposing restrictions on the collection of sensitive information, the NPPs also provide some further limited protections in relation to the use and disclosure of sensitive information. As discussed in Chapter 25, NPP 2, which permits use and disclosure of personal information, sets a more stringent requirement in respect of the use and disclosure of sensitive information under one of its limbs. Where personal information is to be used or disclosed for a purpose other than the primary purpose of collection, that other purpose is to be related to the primary purpose of collection. In the case of the use or disclosure of sensitive information, however, that other purpose must be *directly* related to the primary purpose of collection.[95]

---

92 Rec 22–2.

93 As discussed in Ch 16, the ALRC is of the view that 'law' for the purposes of this exception includes the orders of courts and tribunals. See Rec 16–1.

94 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), 1.

95 *Privacy Act 1988* (Cth) sch 3, NPP2.1(a).

22.78 NPP 2 also prohibits the use of sensitive information for the secondary purpose of direct marketing.[96] The NPPs, however, do not impose separate requirements for the handling of sensitive information in all aspects of the information cycle.

22.79 The *Privacy Act* also provides, outside the context of the privacy principles, that 'related bodies corporate' cannot share sensitive information in the same way that they may share other personal information.[97]

22.80 Some jurisdictions, like New Zealand, do not distinguish between the treatment of sensitive and non-sensitive personal information.[98] Equally, however, others like the United Kingdom and Germany, have separate provisions for regulating the handling of sensitive and non-sensitive personal information.[99] New South Wales privacy law also distinguishes between the disclosure of sensitive and non-sensitive personal information.[100]

Submissions and consultations

22.81 The ALRC asked in IP 31:

> Should federal privacy principles establish a separate regime for the public and private sectors regulating sensitive information in all aspects of the information cycle, including collection, use, disclosure, storage, access, retention and disposal? If so, what should that regime include?[101]

22.82 A number of stakeholders supported the articulation of rules relating to sensitive information with reference to all aspects of the information cycle.[102] On the other hand, a large number of stakeholders submitted that it would be preferable simply to maintain the status quo.[103] For example, it was submitted that instituting a separate regime for handling sensitive information 'would unnecessarily complicate' this area.[104]

---

96 Ibid sch 3, NPP 2.1(c).
97 Ibid s 13B.
98 See *Privacy Act 1993* (NZ).
99 See *Data Protection Act 1998* (UK) sch 1 (Principle 1), sch 3; *Federal Data Protection Act 1990* (Germany).
100 *Privacy and Personal Information Protection Act 1998* (NSW) ss 18, 19.
101 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–32.
102 Office of the Privacy Commissioner, *Submission PR 215*, 28 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.
103 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007.
104 Australian Federal Police, *Submission PR 186*, 9 February 2007. See also Law Council of Australia, *Submission PR 177*, 8 February 2007.

22.83 In DP 72, the ALRC expressed the preliminary view that, if its other proposals were adopted, it would be unnecessary to make any further provisions in the UPPs or elsewhere in the *Privacy Act* to deal with sensitive information.[105]

22.84 A small number of stakeholders submitted that additional protections should apply to sensitive information at each stage of the information cycle, and not merely at the collection stage.[106] PIAC expressed the view that the consequences of misuse of sensitive information at other stages of the information cycle could be of equal or greater seriousness as at the collection stage.[107]

22.85 Privacy NSW submitted that protection for sensitive information should be addressed in each of the privacy principles. In particular, it expressed the view that consent should be required for primary and secondary uses, disclosures, and cross-border flows of sensitive information. It stated that:

> If an agency or organisation is required to afford sensitive information special protection at the point of collection, then there is surely an equal expectation that the subsequent dealings with that information will also be specially protected.[108]

ALRC's view

22.86 The ALRC acknowledges that sensitive information may, in certain circumstances, warrant additional protection beyond the stage of its collection. This is due largely to the potential harmful consequences of its misuse.

22.87 In other chapters of this Report, the ALRC endorses some additional protections for sensitive information at other stages of the information cycle. Namely, the ALRC expresses the view that:

- The limb of the 'Use and Disclosure' principle, which deals with use and disclosure of personal information for a purpose other than the primary purpose of collection, should continue to require a direct relation between the primary purpose of collection and the proposed purpose of use or disclosure where the information is sensitive.[109]

- The 'Direct Marketing' principle should restrict the ability of an organisation to use sensitive information without consent for the purpose of direct marketing,

---

105 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), [19.24], [19.30]–[19.34].

106 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007. See also Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

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

109 See Ch 25 and UPP 5.1(a).

where it proposes to market to non-existing customers or persons under the age of 15 years.[110]

- In interpreting the obligation in the 'Data Security' principle for agencies and organisations to take reasonable steps to protect personal information from misuse and loss, whether a particular security measure is determined to be 'reasonable' will depend on many factors, including the sensitivity of the information.[111]

- The OPC should develop and publish guidance about the 'reasonable steps' agencies and organisations should take to prevent misuse and loss of personal information, which addresses the factors to be taken into account in determining what are 'reasonable steps', including the sensitivity of the information.[112]

- The OPC should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*.[113] This guidance should assist agencies and organisations in understanding consent as it applies to the use, disclosure and transfer overseas, of sensitive information.[114]

- Health information, which is a particularly important type of sensitive information, should be regulated separately by the new *Privacy (Health Information) Regulations*, rather than being dealt with under the UPPs. These Regulations will specify rules tailored to this particular type of sensitive information.[115]

22.88 In light of the above, it is unnecessary to include any further provisions in the model UPPs to deal with sensitive information.

---

110 See Ch 26 and UPP 6.2(a).
111 See Ch 28.
112 See Ch 28 and Rec 28–3.
113 See Ch 19 and Rec 19–1.
114 See UPPs 5.1(b) and 11.(1)(b).
115 See Pt H, especially Chs 60, 63.

23. Notification

Contents

Introduction

23.1 The privacy principles in the *Privacy Act 1988* (Cth) regulating the collection of personal information provide that, in certain circumstances, agencies and organisations are required to ensure that an individual whose personal information has been, or is to be, collected, is aware of a number of specific matters. For convenience, the ALRC, at times, refers to these requirements as ones relating to 'notification'. The relevant principles do not refer expressly to an obligation to notify. One way of ensuring awareness, however, is through notification.

23.2 This chapter considers whether the requirements relating to notification should be set out in a separate privacy principle. It also considers the nature and timing of the obligation to notify, and the circumstances in which such an obligation should arise.

Finally, the chapter addresses the specific matters that should be brought to an individual's attention when his or her personal information is collected.

Current coverage by IPPs and NPPs

23.3 Currently, the requirements relating to notification are dealt with in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) that deal with the collection of personal information. IPP 2 provides that where an agency solicits personal information directly from the individual concerned for inclusion in a record or in a generally available publication, it must take reasonable steps to ensure that, before or as soon as practicable after the information is collected, the individual is generally aware of:

- the purpose for which the information is being collected;
- if applicable, the fact that the collection is authorised or required by law; and
- to whom it is the agency's usual practice to disclose or pass on personal information of the kind collected.

23.4 Similarly, NPP 1.3 provides that an organisation only may collect personal information from an individual after taking reasonable steps to ensure the individual is aware of: the organisation's identity and contact details; the fact that he or she can access the information; the purposes of collection; the organisations to whom the organisation usually discloses information of that kind; any law requiring the particular information to be collected; and the main consequences for the individual if the information is not provided. When an organisation collects personal information from someone other than the individual, NPP 1.5 imposes an obligation to ensure that the individual to whom the information relates is aware of the matters mentioned in NPP 1.3.

Location of notification requirements: separate principle?

23.5 The ALRC examined whether the notification requirements in the model Unified Privacy Principles (UPPs) should be set out in the 'Collection' principle, or dealt with in a separate privacy principle.

23.6 There is precedent for dealing with notification requirements in a separate privacy principle. Notification is treated as a separate privacy principle, for example, in the Asia-Pacific Economic Cooperation *Privacy Framework* (2005),[1] and the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing*

1 See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle II.

of Personal Data and on the Free Movement of Such Data (1995).[2] In some jurisdictions, however, notification requirements are located within the privacy principle dealing with collection of personal information.[3]

Submissions and consultations

23.7 In response to the Issues Paper, *Review of Privacy* (IP 31),[4] a number of stakeholders submitted that notification requirements should be located in a separate privacy principle that deals with openness[5] and notification.[6] One stakeholder argued that this would facilitate 'a more pragmatic discussion of the desirable levels of awareness, and how and when these can be created'.[7]

23.8 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the UPPs should contain a principle called 'Specific Notification' that sets out the requirements on agencies and organisations to provide specific notification to an individual of particular matters relating to the collection and handling of personal information about the individual.[8]

23.9 Many supported this proposal.[9] Reasons for support included that:

- it was confusing to have notification dealt with in the privacy principle dealing with the collection of personal information;[10]

---

2 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), arts 10–11.

3 See, eg, *Privacy Act 1993* (NZ) s 6, Principle 3.

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

5 In general terms, the openness principles in the IPPs and NPPs require agencies and organisations to make available a document that sets out their policies relating to the management of personal information. Openness is discussed in Ch 24.

6 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; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

7 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

8 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 20–1.

9 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; 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; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; I Graham, *Submission PR 427*, 9 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007; Australian Digital Alliance, *Submission PR 422*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. One stakeholder stated that it 'did not disagree' with the proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

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

- locating notification requirements within the principle dealing with collection of personal information fails to give adequate recognition to the importance of notification;[11]

- it would be inappropriate to deal with 'openness' requirements in the same privacy principle as 'notification' requirements because the requirements have a different emphasis.[12]

23.10 The Office of the Victorian Privacy Commissioner (OVPC), for example, stated that:

> Notice statements under a 'Specific Notification' privacy principle are generally more tailored to the particular collection practice, as opposed to the more general statements about all types of information handling practices that organisations engage in, as required under an 'openness' privacy principle.[13]

23.11 Some stakeholders expressed qualified support for the proposal on the basis that the notification principle should include an exception to allow law enforcement bodies to perform their functions properly.[14]

23.12 A comparatively small number of stakeholders, however, opposed the proposal outright.[15] Reasons for opposing it included that:

- there are benefits in retaining the notification requirements in the principle dealing with collection of personal information because it is at this stage of the information cycle that the obligations are triggered;[16]

- it aids compliance to have the notification requirements contained with the collection principle because it reminds agencies and organisations that when they collect personal information they have to meet certain notification requirements;[17]

- it is unclear, in practical terms, how the introduction of a separate principle dealing with notification reconciles with the principles relating to collection and openness;[18]

---

11 Ibid.

12 Ibid; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. See also Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

13 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

14 Australian Federal Police, *Submission PR 545*, 24 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007.

15 Confidential, *Submission PR 570*, 13 February 2008; Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Confidential, *Submission PR 536*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; National Australia Bank, *Submission PR 408*, 7 December 2007.

16 Confidential, *Submission PR 570*, 13 February 2008.

17 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008

18 Ibid; National Australia Bank, *Submission PR 408*, 7 December 2007.

- it would increase the costs and burden of compliance;[19] and
- the approach is inconsistent with a 'light-touch' approach to privacy regulation.[20]

ALRC's view

23.13 The requirements on agencies and organisations to notify or otherwise ensure an individual's awareness of particular matters relating to the collection or handling of an individual's personal information should be consolidated in a single, discrete privacy principle. Notification promotes transparency about an entity's collection and handling of personal information. It is essential in informing individuals about the treatment of their personal information, and their rights in this regard. Dealing with notification in a separate principle, therefore, acknowledges the importance that it plays in the information cycle.

23.14 Concerns about the compliance costs and burden associated with the notification requirements are directed more appropriately to the content of any such requirements, rather than their location.[21] Similarly, stakeholders' views about the need for an exception in the law enforcement context do not impact on the location of the requirements. They are relevant to considering the broader issue of when the obligation to notify arises.

23.15 The different conceptual nature and focus of the requirements relating to notification and openness render them unsuitable to be located within the one privacy principle. On one hand, the openness principles require individuals to be informed about the *general* practices of an agency or organisation relating to the handling of personal information. As such, these requirements apply regardless of whether the agency or organisation has actually collected personal information from a particular individual, or whether the agency or organisation simply might do so in the future. On the other hand, the notification principles apply when personal information has been, or will soon be, collected from a particular individual. Consequently, these principles require the agency or organisation to notify an individual about how it will handle the individual's actual personal information or personal information of the kind collected from the individual.

---

19 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007. Two stakeholders that did not oppose the proposal also noted that agencies would need to be given significant additional resources to comply with the proposed notification requirements: Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

20 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

21 The content of the 'Notification' principle is discussed below.

23.16 It is artificial, however, to regard the operation of the notification and openness principles separately from each other. To do so could duplicate unnecessarily the requirements imposed on agencies and organisations. This is borne out more fully in the discussion below.

Recommendation 23–1 The model Unified Privacy Principles should contain a principle called 'Notification' that sets out the requirements on agencies and organisations to notify individuals or otherwise ensure they are aware of particular matters relating to the collection and handling of personal information about the individual.

Nature and timing of notification obligation

23.17 The current obligations in the IPPs and NPPs do not refer specifically to an obligation to notify individuals. The obligation is to take steps to ensure that an individual is aware of specified matters.

23.18 An agency is currently obliged to take such steps before it collects personal information or, if that is not practicable, as soon as practicable after the information is collected.[22] An organisation is currently obliged to take such steps at or before the time of collection or, if that is not practicable, as soon as practicable after collection.[23]

23.19 Guidance issued by the Office of the Privacy Commissioner (OPC) on the obligation in the NPPs states, in part, that:

> An organisation could put off giving NPP 1.3 information until after the time of collection if there are practical problems in doing so that the organisation cannot overcome by any reasonable means.[24]

23.20 The OPC's guidance sets out a number of factors to be considered in assessing whether it is impracticable to notify individuals of relevant matters at or before the time of collection. These include, for example, the sensitivity of the information; the privacy implications for the individual of not receiving the information at or before collection; what is accepted as industry practice by consumers and industry; and the cost of providing the information at or before collection.[25]

Submissions and consultations

23.21 In DP 72, the ALRC proposed that agencies and organisations should take reasonable steps to ensure that an individual is aware of a number of specified matters

22 *Privacy Act 1988* (Cth) s 14, IPP 2.
23 Ibid sch 3, NPP 1.3.
24 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 28.
25 Ibid, 28.

relating to the collection of his or her personal information. The ALRC proposed that such an obligation should arise at or before the time an agency collects personal information or, if that is not practicable, as soon as practicable after collection.[26]

Nature of obligation

23.22 A number of stakeholders expressed the view that the principle should refer expressly to a requirement to notify individuals of the specified matters.[27] The Public Interest Advocacy Centre (PIAC), for example, submitted that:

> The focus on the individual's awareness is potentially problematic. 'Awareness' is a difficult concept to prove as it involves making assumptions about what was in the individual's consciousness at a particular time. This will inevitably involve some degree of subjectivity. A better test would be to look at whether the individual had, in fact, been notified. This will be easier to prove from an enforcement point of view.[28]

23.23 The Australian Privacy Foundation came to a similar conclusion, but for different reasons. It stated that:

> We are concerned that leaving the obligation as 'ensuring awareness' (as in NPP 1.3) is too open to abuse. For instance … data users could deliberately omit privacy notices from routine communications even where there is minimal marginal cost in repeating it, relying instead on an initial communication constituting 'reasonable steps'…
>
> We agree that the objective of this principle is to ensure awareness, but a better way of consistently achieving this objective would be, in our view, to change this principle from one of reasonable steps to 'ensure awareness' to reasonable steps to specifically 'notify', with a conditional exception where the data user could establish that at least the typical data subject had been made aware by other means.[29]

23.24 The Australian Bankers' Association (ABA), on the other hand, emphasised that an individual could be made aware of matters, other than by way of notification. For example, it stated that the requirement to ensure awareness could be met if an individual was aware of information in a bank's Privacy Policy.[30]

Timing of obligation

23.25 PIAC expressed concern that, under the proposed approach, an individual may sometimes not be made aware of the specified matters until after his or her personal information has been collected. It stated:

---

26 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2, 20–5.

27 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.

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

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

30 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

> The circumstances in which notification after the time of collection will be acceptable should be very limited. Strong justification should be necessary where notice is not provided before or at the time of collection.[31]

23.26 The Cyberspace Law and Policy Centre supported the proposal relating to the time at which the obligation to is to arise. It submitted, however, that the OPC should be required to issue guidance about the 'limited circumstances in which "after the event" notification is acceptable'.[32] It stated:

> Clearly, the objective of awareness—to put the individual in a position of knowledge before they decide whether to give up their personal information—is severely compromised if the information is not provided beforehand. On the other hand, there clearly are some circumstances where it is simply not practicable to convey all or, in some cases, any of the information in advance. The risk of providing an 'if impracticable then later' exception is that it can be abused, with data users who could provide the information prior to collection, perhaps with some cost or creativity, spuriously claiming 'impracticability'.[33]

ALRC's view

Nature of obligation

23.27 An agency or organisation should be required to notify or otherwise ensure that an individual is aware of specified matters relating to the collection of his or her personal information. Notification is one way of ensuring awareness. It is clearly appropriate to refer expressly to notification in the context of the 'Notification' principle.

23.28 Agencies and organisations, however, should be able to rely on other means of ensuring that an individual is aware of specified matters. To insist on notification in every case would be prescriptive. It could increase unnecessarily the compliance burden and costs, as well as overloading individuals with information of which they are already aware.

23.29 For example, a collecting agency or organisation could make inquiries or otherwise satisfy itself that an individual has been made aware of the specified matters by the agency or organisation which disclosed the information to it. This is consistent with the approach in the Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000, which stated:

> If organisation A collected information from an individual, and organisation A usually discloses that type of information to organisation B, then at the very minimum, organisation A would be required to tell the individual that it usually discloses the information to organisation B … Before organisation B could collect the information it would need to be satisfied that the individual was aware of the other [specified] matters as they pertain to organisation B. *If organisation A has given these details to*

---

31 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
32 Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
33 Ibid.

> *the individual, then organisation B does not have to do any notifying itself … The aim of [the requirement] in NPP 1.5 is to ensure that the individual knows what happens to his or her personal information.*[34]

23.30 In other circumstances, it may be legitimate for an agency or organisation to ensure that an individual is aware of specified matters by alerting the individual to specific sections of its Privacy Policy or other general documents containing relevant information. As discussed below, avoiding duplication of material in privacy notices and Privacy Policies reduces compliance costs, and may also have the benefit of reducing unnecessary detail in privacy notices.

23.31 The OPC should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. This guidance should address the circumstances in which an agency or organisation can comply with specific requirements under the 'Notification' principle by alerting an individual to specific sections of its Privacy Policy or other general documents containing the requisite information.

Timing of obligation

23.32 The obligations under the 'Notification' principle should be complied with before or at the time an agency or organisation collects personal information or, if that is not practicable, as soon as practicable thereafter.

23.33 Ideally, agencies and organisations should endeavour to comply with the principle before, or at, the time of collecting personal information. This maximises the potential for an individual to make an informed choice before relinquishing his or her personal information.

23.34 It would be prescriptive and unreasonable, however, to insist that, in all circumstances, the requirement be met before or at the time of collection. The 'Notification' principle needs to be flexible enough—as are the current obligations in the IPPs and NPPs—to adapt to circumstances in which compliance before, or at, the time of collection, is impracticable. Agencies and organisations will need to demonstrate the basis upon which impracticability is asserted, if the issue arises.

Circumstances in which notification obligations arise

23.35 The specific content of notification obligations to be imposed on agencies and organisations is discussed separately below. In general terms these address the fact, and purposes, of collection; usual disclosure practices; and an individual's rights relating to his or her personal information.

---

34 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [338] (emphasis added).

23.36 An initial question that arises, however, is in what circumstances should an agency or organisation be required to notify individuals or otherwise ensure that they are aware of particular matters relating to the collection and handling of their personal information? A consideration of this issue also involves an assessment of whether:

- there need to be exceptions to the circumstances in which the obligations will ordinarily be assumed to arise; and

- an obligation to notify should be imposed on agencies and organisations when they collect personal information from someone other than the individual concerned.

23.37 Each of these issues is considered below.

Reasonable steps

Background

23.38 Currently, when an organisation collects personal information, either from the individual concerned or a third party, it is required to take 'reasonable steps' to ensure that the individual from whom the organisation collects the information is aware of certain specified matters.[35] There is some uncertainty over what is meant by the term 'reasonable steps' and, especially, whether an organisation legitimately may conclude that, in certain circumstances, it would be reasonable to take no steps.

23.39 For example, the OPC review of the private sector provisions of the *Privacy Act 1988* (OPC Review) stated that it would be reasonable to take no steps to provide notice where significant cost or difficulty is involved in contacting a third party whose information has been collected incidentally, or in many circumstances where the information is collected from a public source.[36] The OPC Review recommended that the legislation be amended to make it clear that that there are situations in which the reasonable steps an organisation might take to provide notice to an individual may equate to no steps.[37]

23.40 The OPC's guidance on the meaning of 'reasonable step' provides, in part, as follows:

> Where the circumstances of collection make a matter listed in NPP 1.3 obvious, the 'reasonable steps' might not involve any active measures because the circumstances speak for themselves. For example, in many cases, the identity of the organisation collecting the personal information could be obvious from the circumstances. It may be less obvious on the Internet and when other electronic technologies are used …

---

35 See *Privacy Act 1988* (Cth) sch 3, NPP 1.3, 1.5.

36 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 260.

37 Ibid, rec 75. Professor Roger Clarke has expressed a similar view: R Clarke, 'Serious Flaws in the National Privacy Principles' (1998) 4 *Privacy Law & Policy Reporter* 176, 179.

> Deciding what are reasonable steps involves balancing a number of possible factors, including the importance to the individual of having the relevant knowledge and the cost to the organisation in providing that information.[38]

23.41 Currently, the corresponding obligation imposed on agencies is to 'take such steps (if any) as are, in the circumstances, reasonable to ensure that' the individual concerned is generally aware of specified matters.[39] It is clear, therefore, that in respect of the obligations imposed on agencies it might be reasonable to take no steps to provide notice.[40] The privacy legislation of New Zealand also frames the relevant obligation in this way,[41] but sets out expressly a number of circumstances in which an agency is not required to take any such steps. These circumstances include, for example:

- if the agency, on a recent previous occasion, has taken those steps in relation to the collection of personal information from an individual, involving notification of the 'same information or information of the same kind';
- if the agency believes, on reasonable grounds that:
  - non-compliance would not prejudice the interests of the individual concerned;
  - non-compliance is necessary for law enforcement purposes;
  - non-compliance is authorised by the individual concerned; or
  - compliance would prejudice the purposes of the collection; and
- either the information will:
  - not be used in a form in which the individual concerned is identified; or
  - will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.[42]

---

38 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 28–29.

39 *Privacy Act 1988* (Cth) s 14, IPP 2.

40 The OPC's guidance on IPP 2 provides expressly that 'an agency does not have to give details if giving the details would defeat the purpose of collecting the personal information': Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 15.

41 *Privacy Act 1993* (NZ) s 6, Principle 3(1).

42 See Ibid s 6, Principle 3(3)–(4).

Submissions and consultations

23.42 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to clarify that there may be circumstances in which it is reasonable for organisations to take no steps to ensure that an individual is aware of specified matters relating to the collection of personal information.[43]

23.43 A large number of stakeholders supported such an amendment.[44] Some stakeholders provided examples of circumstances in which it would be reasonable for an organisation to take no steps to notify an individual. These included the following:

- where an organisation receives information from a related body corporate, especially if the individual would reasonably expect the information to be shared in this way;[45]
- where an insurer collects information about the medical history of family members of an individual client;[46]
- where notifying an individual that information about the individual has been collected as part of an alternative dispute resolution scheme may put at risk the safety of third parties;[47]
- in the context of 'family, social or medical history-taking';[48] and
- in the course of an investigation into possible wrongdoing.[49]

23.44 Some stakeholders, however, submitted that no amendment was needed to the 'reasonable steps' requirement. The Australian Privacy Foundation submitted that an amendment which clarified that taking no steps could be reasonable 'would invite self serving interpretation to avoid giving notice even where it was both reasonable and

---

43 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–2.

44 See, eg, Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; ANZ, *Submission PR 173*, 6 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; Investment and Financial Services Association, *Submission PR 122*, 15 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; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93*, 15 January 2007.

45 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. A similar example given is where personal information is disclosed to a contracted service provider: Law Council of Australia, *Submission PR 177*, 8 February 2007.

46 AXA, *Submission PR 119*, 15 January 2007.

47 Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93*, 15 January 2007. See also National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.

48 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007. See also the more detailed discussion of this issue in Part H.

49 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

practicable'.[50] DLA Phillips Fox submitted that NPP 1.3 already sets out 'an objective test of what is reasonable in the circumstances'.[51]

23.45 Telstra suggested that the OPC should issue detailed guidelines on what steps are required to provide notification in various circumstances.[52] The Law Council of Australia submitted that, if a person relies on advice from the OPC that no steps are required, then this should be a full defence if a complaint is later made about the person.[53]

23.46 In DP 72, the ALRC proposed that the OPC provide guidance on the meaning of the term 'reasonable steps' in this context.[54] This proposal was generally supported.[55] Medicare Australia stated that the guidance should make it clear that there are circumstances in which it could be reasonable for no steps to be taken.[56] Some stakeholders that supported the proposal also expressed support for legislative clarification. For example:

- The OPC submitted that the words 'if any' should be added after 'reasonable steps', to make it clear that the taking of no steps could be reasonable.[57]

- The Australian Privacy Foundation submitted that 'far more of the detail of what the requirements mean in practice should be incorporated in the principle itself, leaving less to be covered in guidance'.[58]

- The National Health and Medical Research Council (NHMRC) submitted that the new *Privacy (Health Information) Regulations* should provide that individuals need not be notified when personal information is collected in confidence. It also submitted that the new regulations or the proposed guidance should specify that it would be reasonable to take no steps to notify an individual about the collection of his or her personal information, where the

---

50 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.
51 DLA Phillips Fox, *Submission PR 111*, 15 January 2007.
52 Telstra, *Submission PR 185*, 9 February 2007.
53 Law Council of Australia, *Submission PR 177*, 8 February 2007.
54 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 20–7.
55 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; 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; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. One stakeholder stated that guidance, jointly produced by state and territory privacy commissioners, would be useful: Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.
56 Medicare Australia, *Submission PR 534*, 21 December 2007.
57 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. Another stakeholder also submitted that it should be made clear that 'there are circumstances in which no notification is required to be given': GE Money Australia, *Submission PR 537*, 21 December 2007.
58 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.

information was collected in the context of taking a family, medical or social history, or in relation to quality assurance and approved research activities.[59]

23.47 PIAC, however, expressed the view that, while guidance on the meaning of 'reasonable steps' in the context of the notification requirements is necessary, it is preferable for such guidance to be included in the *Privacy Act*, regulations or in binding codes.[60]

ALRC's view

23.48 The *Privacy Act* should make it clear that there may be circumstances where it will be reasonable for an agency or organisation to take no steps to notify or otherwise ensure that an individual is aware of specified matters resulting from the collection of his or her personal information. The 'Notification' principle, therefore, should provide expressly that an agency or organisation is obliged to take 'such steps, if any, as are reasonable in the circumstances' to notify or otherwise ensure that an individual is aware of specified matters. Such an approach is consistent with that currently adopted in the IPPs and the privacy legislation of New Zealand.

23.49 Providing legislative clarification in this regard is essential to address the confusion caused by the fact that use of the phrase 'must take reasonable steps' in NPP 1 appears to imply that some *active* steps must be taken by an organisation when collecting personal information. This is despite the fact that, in certain circumstances, logic dictates that it would be reasonable for no steps to be taken.

23.50 In addition to legislative clarification, the OPC should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. The guidance should address specific circumstances when it would be reasonable for no steps to be taken to notify individuals about the collection of their personal information. In this regard, the guidance should address areas identified by stakeholders as needing clarification,[61] as well as areas currently recognised in other jurisdictions as properly being excluded from the ambit of the obligation to take reasonable steps. The guidance should address, therefore, circumstances when:

- notification would prejudice the purpose of collection, for example, when it would prejudice:
  - the prevention, detection, investigation and prosecution of offences, breaches of a law imposing a penalty or seriously improper conduct;
  - the enforcement of laws; or

---

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

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

61 Many of the views expressed by stakeholders about areas requiring clarification are set out below, particularly in discussions which consider the issue of exceptions to the 'Notification' principle.

- the protection of the public revenue;

- collection of personal information is required or authorised by or under law for statistical or research purposes;
- the personal information is collected from an individual on repeated occasions;
- an individual has been made aware of the relevant matters by the agency or organisation which disclosed the information to the collecting agency or organisation;
- non-compliance with the principle is authorised by the individual concerned;
- non-compliance with the principle is required or authorised by or under law;
- notification would pose a serious threat to the life or health of any individual; and
- health services collect family, social or medical histories.[62]

Should there be exceptions or other qualifications to the principle?

Background

23.51 The ALRC examined whether the 'Notification' principle should set out the circumstances in which an agency or organisation will not be required to comply.

23.52 Currently, the IPPs do not provide for any exceptions to the notification requirements as they apply to the collection of personal information by agencies. Similarly, the NPPs do not provide for any exceptions to the notification requirements as they apply to the collection of personal information by organisations directly from the individual concerned. The NPPs do provide, however, that where an organisation collects personal information about an individual from someone another than the individual concerned, the notification requirements apply 'except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual'.[63]

23.53 As noted above, the privacy legislation of New Zealand sets out a number of exceptions to the notification requirements within the body of the principle dealing with collection of personal information.

---

62 This is considered further below in the discussion about collection of personal information from third parties.

63 *Privacy Act 1988* (Cth) sch 3, NPP 1.5.

23.54 In DP 72, the ALRC proposed a number of exceptions to the 'Notification' principle. In addition, stakeholders made submissions about the creation of other exceptions. These are addressed separately below.

Submissions and consultations

Required or specifically authorised by or under law

23.55 In DP 72, the ALRC proposed that agencies that collect personal information—whether directly from an individual or from someone other than the individual—should not be required to comply with the notification requirements if they are required or specifically authorised by or under law not to make the individual aware of one or more of the matters to be notified.[64]

23.56 Many stakeholders supported the proposal.[65] Some submitted that the application of the proposed exception should be extended to cover organisations, in addition to agencies.[66] Other stakeholders opposed the proposal.[67] The OPC, for example, submitted that such an exception would be unnecessary if the principle stipulates expressly that it might be reasonable to take no steps to comply. It stated that such an approach would provide adequately for circumstances 'where notification would be counter to the functions of an agency'.[68]

23.57 A number of stakeholders submitted that the exception is insufficient in itself to enable agencies to exercise their functions. These stakeholders submitted that 'other public interest' exceptions to the principle are required to:

- enable agencies involved in law enforcement, intelligence, investigations or complaint handling to perform properly all of their functions;[69]

---

64 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–4, 20–5(b)(iii).

65 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; GE Money Australia, *Submission PR 537*, 21 December 2007; Optus, *Submission PR 532*, 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; 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.

66 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; GE Money Australia, *Submission PR 537*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australian Finance Conference, *Submission PR 398*, 7 December 2007.

67 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.

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

69 Australian Federal Police, *Submission PR 545*, 24 December 2007; Human Rights and Equal Opportunity Commission, *Submission PR 500*, 20 December 2007; Confidential, *Submission PR 448*, 11 December 2007. The Queensland Government stated that 'it would be counter-productive to require … notice to be given where the information was legitimately collected as part of law enforcement activities without the individual being aware': Queensland Government, *Submission PR 490*, 19 December 2007.

- prevent an impediment, or prejudice, to an investigation;[70]
- allow investigations into collection of revenue that an agency is authorised to collect and recover, such as child support payments;[71] and
- protect the public revenue.[72]

23.58 A number of stakeholders expressed concern about the proposed requirement that an agency be 'specifically authorised' by or under law not to make the individual aware of certain matters.[73] Stakeholders noted the absence of laws that specifically authorise non-compliance with the matters proposed to be the subject of the notification requirements.[74]

23.59 Medicare Australia submitted that such a requirement 'could have implications for the effective administration of government programs, especially our compliance and investigation functions'.[75] The Australian Federal Police (AFP) stated that:

> The use of the word '***specifically***' assumes that all the powers and functions of an agency will always be set out expressly in the legislation. However, practical experience demonstrates that the legislation does not always address every issue and it is sometimes necessary to determine what is required by necessary implication as well as by what is expressed.[76]

Reasonable expectations

23.60 In DP 72, the ALRC proposed that agencies and organisations that collect personal information—whether directly from an individual or from someone other than the individual—should be required to comply with the notification requirements only in circumstances where a reasonable person would expect to be notified.[77]

23.61 Some stakeholders expressed concerns about this proposed qualification on the basis that it is unnecessary and would lower privacy protections by introducing an additional 'reasonableness' test.[78] For example, the OPC expressed concern that

---

70 Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.
71 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007
72 Australian Government Centrelink, *Submission PR 555*, 21 December 2007.
73 Australian Federal Police, *Submission PR 545*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.
74 Confidential, *Submission PR 488*, 19 December 2007; Confidential, *Submission PR 448*, 11 December 2007.
75 Medicare Australia, *Submission PR 534*, 21 December 2007.
76 Australian Federal Police, *Submission PR 545*, 24 December 2007.
77 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(1); 20–5(b)(i).
78 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

> the introduction of the proposed 'reasonable person test' establishes a threshold test for agencies and organisations to determine whether they are under an obligation to provide specific notification. Only once they have determined that the notification requirements are applicable to the circumstances, do they then need to consider what might constitute 'reasonable steps'. As such, the Office is concerned that [it] effectively establishes a mechanism by which agencies and organisations can exclude themselves from their notification obligations entirely.[79]

23.62 Other stakeholders raised concerns about the practicalities of applying a 'reasonable person' test. In particular:

- The Department of Agriculture, Fisheries and Forestry stated that it was likely to be unclear when a 'reasonable person' would expect to be notified.[80]

- The Australian Taxation Office (ATO) expressed the view that the application of a reasonable person test could be problematic in circumstances where it receives anonymous information about taxpayers. While such information is important, for example, in the identification of potential tax avoidance schemes, the ATO noted that a 'reasonable person' might expect to be notified of the receipt of such information in order to rebut its content or implications.[81]

23.63 The Australian Privacy Foundation submitted that the qualification should be redrafted to make it a subjective, rather than objective, test. It suggested that an agency or organisation should comply with the notification requirements unless 'it reasonably believes that there is a reasonable expectation on the part of individuals that they not be notified'.[82]

Threat to individual's health and life

23.64 In DP 72, the ALRC proposed that agencies and organisations that collect personal information—whether directly from an individual or from someone other than the individual—should be required to comply with the notification requirements except to the extent that making the individual aware of the specified matters would pose a serious threat to the life or health of any individual.[83]

23.65 This proposal received strong support from two stakeholders.[84] Other stakeholders, however, opposed the exception on various grounds. These included that the exception would be addressed adequately by making it clear in the 'Notification'

---

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

80 Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.

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

82 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.

83 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(2); 20–5(b)(ii).

84 Cancer Council Australia and Clinical Oncological Society of Australia, *Submission PR 544*, 23 December 2007.

principle that there might be circumstances where it would be reasonable to take no steps to comply.[85] Further, stakeholders noted that such an exception does not currently apply to the collection of personal information directly from the individuals to whom the information relates. They questioned the policy basis for extending the application of the exception to direct collection.[86] For example, the Australian Privacy Foundation submitted:

> Given that in the direct collection situation the individual will be aware that information is being collected, it seems unlikely that informing them of the [matters to be notified] could cause any additional harm.[87]

23.66 The Department of Foreign Affairs and Trade submitted that this exception should be expanded to include threats to an individual's safety, public health and public safety.[88]

Research and statistics

23.67 The ALRC did not propose in DP 72 that there be an exception to the notification requirement where information is collected for statistical purposes or research. The Australian Bureau of Statistics (ABS) submitted that such an exception is necessary. It stated:

> The ABS … collects information in relation to individuals other than from the individuals themselves. This can be seen, for example, in the Census, where one person in a household may complete the form for the entire household, or the Longitudinal Study of Australian Children … where information in relation to one parent may be provided by the other parent …
>
> [A] requirement to advise the individual concerned when information about them is collected from another person could place an overwhelming administrative burden on the ABS.[89]

23.68 The ABS submitted that there should be an exception similar to that in the privacy legislation of New Zealand. That is, the exception should cover information that will:

- not be used in a form in which the individual concerned is identified; or
- be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.[90]

---

85 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
86 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007.
87 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
88 Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008.
89 Australian Bureau of Statistics, *Submission PR 383*, 6 December 2007.
90 Ibid.

ALRC's view

23.69 The qualification that an agency or organisation need only take such steps, if any, as are reasonable in the circumstances is significant. It enables the 'Notification' principle to be sufficiently high-level and flexible to be applied in a wide variety of circumstances, including those in which notifying an individual of specific matters relating to the collection of his or her personal information would not be reasonable.

23.70 It would be inconsistent with the adoption of high-level principles to introduce detailed and prescriptive rules concerning the application of this requirement. It is inappropriate even to make provision for a very limited number of exceptions to the principle. Such an approach creates a legitimate expectation that other valid circumstances also will be made the subject of an exception. This is likely to result in a proliferation of legislative exceptions, fundamentally at odds with a principles-based approach.[91]

23.71 Rather, as noted above, and consistent with the approach taken with respect to the 'Collection' principle, the OPC should develop and publish focused guidance, which addresses the types of circumstances in which it may be reasonable for an agency or organisation to take no steps to notify individuals about the collection of their personal information. Circumstances identified by stakeholders include where:

- notification would prejudice the purposes of collection, for example in the context of law enforcement; and

- the collection of personal information is required or authorised by or under law for statistical or research purposes.

23.72 The guidance should address circumstances in which not taking any steps to notify individuals about the collection of their personal information is authorised or required by or under law. The ALRC agrees that references to 'specific' authorisations by or under law are unhelpful because of the absence of laws that specifically authorise agencies and organisations not to take any steps to notify individuals about the matters recommended to be the subject of the notification requirements.[92]

23.73 The guidance also should address where notification would pose a threat to an individual's health or safety. Such scenarios are more likely to arise where personal information is collected from third parties, rather than directly from the individual concerned.

23.74 It is also unnecessary and undesirable to qualify the notification requirements by providing that they arise only where a reasonable person would expect to be notified. It

---

91 See Ch 4.
92 See also Ch 16.

is sufficient that the principle provides that agencies and organisations are to take such steps, if any, as are reasonable in the circumstances. To add another test of reasonableness is confusing, and may also have the undesirable consequence of lowering privacy protections.

Collection of personal information from a third party

Background

23.75 The ALRC examined whether agencies and organisations should be required to comply with notification obligations regardless of whether they collect personal information directly from the individual concerned or from someone other than the individual.

23.76 Currently, agencies are obliged to ensure that individuals are aware of specified matters relating to the collection of their personal information only where they solicit the information from the individual concerned.[93]

23.77 In contrast, organisations are under an obligation to ensure individuals are aware of specified matters relating to the collection of their personal information, regardless of whether information is collected directly from the individual or from someone other than the individual.[94]

23.78 OPC guidance provides that the steps that an organisation would need to take to make an individual aware of relevant matters when it does not collect directly from the individual concerned 'will depend on the circumstances'.[95]

23.79 One of the circumstances in which personal information is collected from third parties is in the context of the provision of health services. In this regard the Privacy Commissioner has issued Public Interest Determinations (PIDs), which allow health service providers to collect the personal information of third parties, without their consent, where it is relevant to a health consumer's family, social or medical history.[96] The determinations do not exempt health service providers from notifying third parties of such collection. The Privacy Commissioner has stated, however, that an exemption is not necessary because the obligation imposed on organisations is to be interpreted as meaning that, in some circumstances, no steps need to be taken to notify an individual of the collection of his or her personal information.[97] Further, the OPC Review stated:

> The collection of family, social and medical history information is a critical part of providing assessment, diagnosis and treatment to individuals. The Commissioner

93 *Privacy Act 1988* (Cth) s 14, IPP 2.
94 Ibid sch 3, NPP 1.3, 1.5.
95 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 32.
96 See Privacy Commissioner, *Public Interest Determination 10*, effective 11 December 2007; Privacy Commissioner, *Public Interest Determination 10A*, effective 11 December 2007. These replaced PIDs 9 and 9A, and are discussed in Ch 63.
97 Privacy Commissioner, *Public Interest Determination 10A*, effective 11 December 2007, 9.

> acknowledged that obtaining the consent of third parties to collect their information, and notifying those individuals about these collections, would be impractical, inefficient and detrimental to the provision of quality health outcomes.[98]

Submissions and consultations

23.80 In response to IP 31, a number of stakeholders submitted that agencies and organisations should be required to notify individuals of the collection of personal information regardless of the source of personal information.[99] It was noted that the contrary position would create 'a risk that the intention of ensuring individuals were aware who was collecting their information and its use could be circumvented by using third party information providers'.[100]

23.81 In DP 72, the ALRC proposed that the obligation on agencies and organisations to ensure that an individual is aware of specified matters relating to the collection of personal information, should apply to circumstances where the information is collected from someone other than the individual concerned.[101]

23.82 There was support for this general approach.[102] For example, Carers Australia stated that the proposed approach is important for carers because personal information is sometimes collected without their knowledge in the course of providing a service to a person with a disability, illness or injury. It stated that:

> The Specific Notification Principle will allow carers to access and, if necessary, correct information held about themselves. As noted, such a measure promotes fairness, transparency and accuracy.
>
> Whilst generally welcome, this measure is particularly useful as a safeguard against malicious and/or vexatious claims of abuse, neglect or exploitation allegedly perpetrated by the carer.[103]

---

98 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 274.

99 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; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

100 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

101 See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 20–5.

102 See, eg, Optus, *Submission PR 532,* 21 December 2007; Centre for Law and Genetics, *Submission PR 497,* 20 December 2007; Carers Australia, *Submission PR 423,* 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353,* 30 November 2007. See also Public Interest Advocacy Centre, *Submission PR 548,* 26 December 2007; Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007. The Australian Direct Marketing Association stated that it 'did not disagree' with this proposal: Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007.

103 Carers Australia, *Submission PR 423,* 7 December 2007.

23.83 A number of agencies expressed concerns, however, about the administrative burden and 'prohibitive' cost that would be imposed by requirements relating to notification in circumstances where an agency collects personal information from someone other than the individual.[104] The ABS, for example, expressed concerns relating to the collection of personal information from third parties for statistical purposes.[105] The Department of Foreign Affairs and Trade stated that the proposal was problematic in the context of collecting personal information from third parties for the purpose of passport applications. It stated:

> Most of the 1.4 million passport applications that are lodged each year require an applicant to provide information relating to a third party, such as details of parentage and spouse of the non-lodging parent on a child's application, or guarantor details used to identify applicants. In such cases it would be prohibitively expensive and administratively challenging to advise these third parties of the information required under UPP 3.1.[106]

23.84 The Queensland Government submitted that notification obligations should arise only where an agency solicits personal information.[107] The Department of Defence expressed concern that the proposal could impact adversely on the process of vetting security clearances.[108]

23.85 Some tribunals noted that the proposed extension of the obligations in the IPPs to personal information collected from a third party appeared to be inconsistent with their adjudicative functions.[109]

23.86 Many stakeholders expressed concern about the proposed subject matter of the obligation—in particular, the proposal that an agency or organisation be required to inform an individual of the fact of collection and, on request, the source of personal information. These concerns are addressed separately below.[110]

23.87 In DP 72, the ALRC also proposed that the OPC should provide guidance on the circumstances in which it is necessary for an agency or organisation to notify an individual when it has received personal information about the individual from a source other than the individual concerned.[111]

---

104 See, eg, Australian Government Department of Foreign Affairs and Trade, *Submission PR 563,* 24 January 2008; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559,* 15 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; Australian Bureau of Statistics, *Submission PR 383,* 6 December 2007.

105 Australian Bureau of Statistics, *Submission PR 383,* 6 December 2007.

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

107 Queensland Government, *Submission PR 490,* 19 December 2007.

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

109 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 533,* 21 December 2007.

110 See discussion on subject matter of notification.

111 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 20–6.

23.88 This proposal received general support.[112] Medicare Australia, for example, expressed the view that OPC guidance would need to be tailored to cover specific sectors, and possibly even specific agencies.[113]

23.89 The NHMRC submitted that the guidance or the *Privacy (Health Information) Regulations* should specify that, in the context of taking a family, medical or social history or undertaking approved research activities, it would be reasonable to take no steps to notify the individual to whom the information relates that the information has been collected.[114]

ALRC's view

23.90 Agencies and organisations should be subject to an obligation to notify or otherwise ensure an individual's awareness of specified matters relating to the collection of his or her personal information, regardless of whether that information is collected directly from the individual or from someone other than the individual. Such an obligation is already incumbent on organisations.

23.91 The extension of the scope of the obligation as it applies to agencies will require agencies to consider the circumstances in which the obligations arise. They also will need to assess whether it will be reasonable, in exercising any of their functions, not to take any steps to notify individuals about the collection of their personal information. Again, the qualification that an agency or organisation need only take such steps, if any, as are reasonable in the circumstances is significant. The principle is worded at a sufficiently high level. It is flexible enough to cater for the wide range of circumstances in which agencies and organisations collect personal information from third parties.

23.92 Further, guidance to be developed and published by the OPC to assist agencies and organisations to comply with the 'Notification' principle should address specific circumstances where it would not be reasonable to provide notification where personal information has been collected from a third party. As mentioned above, such circumstances include, where:

---

112 Government of South Australia, *Submission PR 565*, 29 January 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Federal Police, *Submission PR 545*, 24 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; National Legal Aid, *Submission PR 521*, 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; Privacy NSW, *Submission PR 468*, 14 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. Suncorp Metway Ltd opposed the proposal: Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

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

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

- the collection of personal information is required or authorised by or under law for statistical or research purposes;
- notification would pose a serious risk to the life or health of any individual; or
- health services collect family, social or medical histories.

23.93 As discussed in detail below, an agency or organisation that collects personal information from a third party should not be required to inform the individual concerned about the source of the information. This approach is likely to alleviate significantly the concerns expressed about the cost and administrative burden imposed by the notification requirements in the context of indirect collection of personal information.

23.94 Concerns expressed by tribunals about the impact of this requirement on their adjudicative functions are addressed by the ALRC's recommendation to exempt partially tribunals from the operation of the *Privacy Act*.[115]

Subject matter of notification

23.95 Many individuals find general privacy notices confusing, too long and difficult to relate to their particular situation.[116] Professor Fred Cate has criticised modern privacy notices, by stating:

> Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice.[117]

23.96 The ALRC examined the matters in respect of which a person should be notified or otherwise made aware of, at or about the time that his or her personal information is collected.

23.97 As noted above, the IPPs and NPPs currently set out a number of matters about which agencies and organisations are required to ensure that individuals are aware of at or about the time that their personal information is collected. The specified matters share some common ground but are not consistent. Both agencies and organisations are required to ensure that an individual is aware:

- of the purposes for which the information is collected;
- that the personal information collected is required by law; and

---

115 See Rec 35–2.

116 See, eg, Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), 39.

117 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341, 341.

- of the entities to whom personal information of that kind is usually disclosed.

23.98 The two last-mentioned obligations, however, are somewhat different in scope. Agencies are required to ensure that an individual is aware of the *fact* that either a collection of personal information is required *or authorised* by or under law, while organisations are required to ensure that an individual is aware of any *law* that requires the particular information to be collected.

23.99 Agencies are required to ensure that an individual is aware of any entity to which it is the agency's usual practice to disclose personal information of the kind collected.[118] Agencies also are required to ensure that an individual is aware of the usual disclosure practices of the entities to which they disclose, if it is known to them. Organisations, on the other hand, are required only to ensure that an individual is aware of the organisations (or the types of organisations) to which information of that kind is usually disclosed.

23.100 Further, only organisations are obliged to ensure that an individual is aware of the: collector's identity and contact details; fact that the individual is able to gain access to the information; and main consequences of not providing the information.

23.101 In other jurisdictions, such as New Zealand, agencies are required to make an individual aware of the: collector's identity and contact details; fact that the individual can access and correct the information; and consequences for the individual if the information is not provided.[119]

23.102 The discussion below addresses specific categories of matters that potentially could be the subject of a notification requirement.

The fact and circumstances of collection

23.103 Neither the IPPs nor the NPPs require an agency or organisation to notify an individual that it has collected, or is about to collect, personal information about that individual. It is arguably implicit in the existing notification provisions that the agency or organisation needs to provide the individual with notice that his or her personal information has been collected.

23.104 An individual may not always be aware that his or her personal information has been collected. This is so particularly in light of existing and developing technology that allows or facilitates the collection of personal information about an individual without the individual knowing that this has occurred.[120] In response to IP 31, the Victorian Society for Computers and the Law (VSCL) noted that certain

---

118 See *Privacy Act 1988* (Cth) s 14, IPP 2 which refers to 'any person to whom, or any body or agency to which' it is the agency's usual practice to disclose personal information.

119 See *Privacy Act 1993* (NZ) s 6, Principle 3(1)(d), (f), (g).

120 The impact of developing technology on privacy is discussed in Part B.

types of biometric information, such as iris scanning collected for the purposes of inclusion in a biometrics template, are likely to require the active cooperation of the individual in the process of collection. In comparison, biometrics such as facial and voice recognition may be collected without the knowledge or cooperation of the individual.[121]

23.105 The VSCL also noted that rapid developments in technology—including in the field of biometrics systems—may result in the widespread availability of technologies that are capable of collecting personal information without the knowledge of the individual.[122] Other technologies, such as invisible information collecting devices on web pages or hidden radio frequency identification (RFID) tags, already may be collecting personal information without the knowledge of the individuals concerned.

Submissions and consultations

23.106 In DP 72, the ALRC proposed that, where an agency or organisation collects personal information about an individual either directly from the individual or from someone other than the individual, it should be required to take reasonable steps to ensure that the individual is aware of the fact and circumstances of collection (for example, how, when and from where the information was collected).[123]

23.107 Some stakeholders expressed support for the ALRC's approach.[124] Other stakeholders noted that this requirement would be new to both agencies and organisations,[125] and expressed strong concerns about its application. These concerns included that:

- the drafting did not appear to reflect the intention that the obligation should arise only where an individual might not be aware of the collection of his or her personal information;[126]

---

121 Victorian Society for Computers and the Law Inc, *Submission PR 137*, 22 January 2007.

122 Ibid.

123 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(a), 20–5(a)(i).

124 See, eg, Optus, *Submission PR 532*, 21 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Privacy NSW, *Submission PR 468*, 14 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007.

125 Confidential, *Submission PR 536*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.

126 Medicare Australia, *Submission PR 534*, 21 December 2007. Another stakeholder expressed the view that the notification requirements should apply only where 'personal information is clearly sourced via unsolicited means and the person is unaware of the collection of their information' as opposed to circumstances involving 'a relationship formed through solicited means': Australian Unity Group, *Submission PR 381*, 6 December 2007.

- because an individual would generally know if, how, and to whom he or she was providing personal information, the wording should make it clear that this requirement only arises in specific circumstances;[127]

- the obligation, together with others proposed, would: be impractical, costly, inconsistent with environmental and economic objectives; inconvenience customers;[128] and impose a resource intensive burden on agencies;[129]

- the potential additional compliance burden that this obligation would impose is questionable on a costs and benefits analysis;[130]

- the obligation is inconsistent with certain requirements and practices in law enforcement;[131] and

- its application to circumstances where law enforcement agencies obtain personal information about an individual from someone other than the individual, including from anonymous or confidential sources, is problematic.[132]

ALRC's view

23.108 Agencies and organisations should be required to notify or otherwise ensure that an individual is aware of the fact and circumstances of the collection of his or her personal information where the individual may not be aware of such collection. Circumstances of collection may include how and when the information was collected.

23.109 Such an obligation is necessary to address, for example, circumstances where an individual's personal information is collected by technology—such as RFID tags, software such as 'cookies', and biometrics—without the individual's knowledge. It also will be of particular significance where an individual's personal information is collected from a third party, without the individual's knowledge. It is essential that an individual is equipped with knowledge of the fact and circumstances of collection to enable the exercise of any available rights relating to that information, such as those relating to access and correction. Such an approach also promotes transparency in the collection practices of agencies and organisations.

---

127 Australian Government Centrelink, *Submission PR 555,* 21 December 2007. Another stakeholder expressed the view that in the direct collection context there should be no requirement to state that the information was collected from the individual: Law Council of Australia, *Submission PR 527,* 21 December 2007.

128 Confidential, *Submission PR 536,* 21 December 2007.

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

130 Australian Bankers' Association Inc, *Submission PR 567,* 11 February 2008.

131 See, eg, Confidential, *Submission PR 488,* 19 December 2007.

132 See, eg, Australian Government Centrelink, *Submission PR 555,* 21 December 2007; Australian Communications and Media Authority, *Submission PR 522,* 21 December 2007; Australian Taxation Office, *Submission PR 515,* 21 December 2007.

23.110 The obligation, however, should not be imposed on agencies and organisations where it is clear that an individual is aware that his or her personal information has been collected. This would cover many circumstances where individuals provide the information themselves and, therefore, are directly involved in the collection process. The ALRC agrees that providing notification in such circumstances cannot be justified on a cost and benefits basis. Notifying individuals directly involved in the collection process about the fact and circumstances of collection is a process of limited, if any, utility. It delivers little by way of additional privacy protection. Further, the provision of such information could detract the individual's attention from other important information relating to the collection, required to be provided by the agency or organisation, of which he or she is not aware. Imposing an arguably unnecessary requirement on agencies and organisations also would be onerous and costly, adding significantly to their compliance burden.

23.111 Professor Cate has made a similar point:

> If the collection from data subjects is not reasonably obvious, then there should be prominent notice of the fact. If data collection is reasonably obvious, additional notice requirements are superfluous.[133]

23.112 As noted above, an agency or organisation should be required only to take reasonable steps, if any, to notify or otherwise ensure that an individual is aware of the matters the subject of the 'Notification' principle. Where notification of the fact and circumstances of collection would prejudice the purpose of collection, for example, then it may be reasonable for no steps to be taken.

Collector's identity and an individual's rights

23.113 As noted above, only the NPPs contain obligations relating to notification of: a collector's identity; an individual's rights relating to access; and the main consequences of not providing the information.

Submissions and consultations

23.114 In IP 31, the ALRC asked whether these notification obligations should be extended to agencies.[134] In response to IP 31, a majority of stakeholders supported such an amendment to bring the notification requirements of agencies in line with those that currently apply to organisations.[135]

---

133 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (2007) 341, 370.

134 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–3.

135 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; 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; Office of the Information Commissioner

23.115 One stakeholder suggested that such a provision has become necessary because it is now more difficult for individuals to know which government agency they are dealing with, given the 'increasing use of campaign names and brands by the public sector and with ever-changing administrative arrangements and "portfolios"'.[136]

23.116 A small number of stakeholders, however, opposed this approach.[137] One stakeholder argued that it would place an unreasonable impediment on law enforcement agencies.[138]

23.117 In DP 72, the ALRC proposed that where an agency or organisation collects personal information about an individual either directly from the individual or from someone other than the individual, it should be required to take reasonable steps to ensure that the individual is aware of: the identity and contact details of the agency or organisation; the fact that the individual is able to gain access to the information; and the main consequences of not providing the information.[139]

23.118 The Cyberspace Law and Policy Centre supported the inclusion of all of these matters. It also suggested that the 'Notification' principle should require that the contact details provided are to be 'functional'.[140]

23.119 A number of stakeholders expressed the view that the notification requirement relating to access also should refer specifically to the ability of an individual to seek correction of his or her personal information.[141]

ALRC's view

23.120 Agencies should be subject to the same notification requirements that apply to organisations. There are compelling policy reasons, essentially based on fairness, to justify the imposition of an obligation on agencies and organisations to notify the individuals from whom they collect personal information of their identity and contact details. It is implicit that the contact details to be provided should be functional. In other words, individuals should know who to contact in order to exercise any rights that they may have relating to their personal information, and the means by which contact can be made.

(Northern Territory), *Submission PR 103*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007.

136 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

137 Australian Federal Police, *Submission PR 186*, 9 February 2007; Confidential, *Submission PR 165*, 1 February 2007; Australian Government Department of Families, Community Services and Indigenous Affairs, *Submission PR 162*, 31 January 2007.

138 Confidential, *Submission PR 165*, 1 February 2007.

139 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(b), (c), (e); 20–5(a)(i).

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

141 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.

23.121 It is important and fair for individuals also to be informed of their rights of access to, and correction of, personal information, as provided for in the UPPs.[142] The provision of such information promotes accountability and transparency. Informing individuals of their rights relating to access and correction arguably increases the likelihood that individuals will exercise those rights in order to check the accuracy of their personal information. Such notification, therefore, may assist agencies and organisations in complying with their obligations to ensure that the personal information they collect is accurate, complete, up-to-date and relevant under the 'Data Quality' principle.[143]

23.122 Individuals also should be informed of the main consequences of not providing personal information, regardless of whether the entity seeking the information is an agency or organisation. For example, it would be important for an individual to be informed that the failure to provide an agency with personal information will result in the withholding of a service or benefit.

Purposes for which information is collected

23.123 As noted above, both the IPPs and NPPs require agencies and organisations to ensure that an individual generally is aware of the purposes for which the information is collected.

23.124 The OPC's guidance on the relevant obligation in the IPPs provides that:

> The Privacy Commissioner usually interprets the purpose of collection narrowly. For example, the Privacy Commissioner normally does not accept the view that an agency collects personal information just to administer an agency or a set of laws. The purpose of collection should be more specific than this and it should relate to the current reason for collecting the information … [144]
>
> Normally the purpose of collection depends on the reason the agency is collecting the personal information at the time it collects the information. However, sometimes the agency knows the information will be used for other purposes. If so, the agency should normally tell the person about the other uses when it collects the information.[145]

23.125 The OPC's guidance on the equivalent obligation in the NPPs states that:

> An organisation could keep the description of the purposes reasonably general as long as the description is adequate to ensure that the individual is aware of what the organisation is going to do with information about them. The organisation does not

142 The mechanics of exercising rights of access to, and correction of, personal information, however, should be addressed in an agency's or organisation's Privacy Policy: see Ch 24.

143 The 'Data Quality' principle is discussed in Ch 27.

144 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 6.

145 Ibid, 16.

> have to describe internal purposes that form part of normal business practices, such as auditing, business planning or billing.[146]

Submissions and consultations

23.126 In DP 72, the ALRC proposed the retention of a requirement relating to notification of the purposes of collection of personal information by agencies and organisations, whether the collection is directly from the individual concerned, or from someone other than the individual.[147]

23.127 Two agencies submitted that the proposal concerning the specification of purpose was problematic.[148] Medicare Australia stated:

> There is a challenge with expressing 'purposes' of collection in privacy notes for agencies like Medicare Australia. The information is often collected to administer one particular program, but that same information is also relevant to other programs which the individual is participating in (either at that time or as new government programs or incentives are added). To reduce the burden on both the individual and the agency, the notification requirement needs to encompass that the information may be used for related purposes, which would remove the necessity of repeatedly having to collect the same information or seek new consent for use, especially where we believe the individual would expect us to use their information to update the relevant parts of programs they are participating in.[149]

23.128 The ATO stated:

> In some circumstances the [ATO] collects information initially for the purpose of making an assessment or amended assessment but after analysis of the information the purpose changes and prosecution or other civil action is initiated … Proposal 20–2 does not appear to address this situation of subsequent change of purpose.[150]

ALRC's view

23.129 Agencies and organisations should continue to be obliged to notify or otherwise ensure that the individuals from whom they collect personal information are aware of the purposes for which the information is collected. There is no policy reason to amend or remove this requirement.

23.130 The concerns expressed by agencies about complying with this requirement appear to be addressed by OPC guidance. To the extent that agencies and organisations know at the time of collection that they intend to use the personal information for purposes related to the purpose of collection, those related purposes also should be the subject of notification. This would not extend, however, to a situation, such as that

---

146 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 30.

147 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(d); 20–5(a)(i).

148 Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007.

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

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

described by the ATO, where an agency collects personal information for a purpose unrelated to law enforcement but *subsequently* forms the intent to use the information for a purpose related to law enforcement. Such use would, however, be authorised under the 'Use and Disclosure' principle in the model UPPs.[151]

Entities to which information usually disclosed

23.131 As noted above, the obligations imposed on agencies and organisations respectively to ensure individuals are aware of the entities to which they usually disclose personal information of the kind collected, are different in scope.

23.132 Specifically, NPP 1.3 requires an organisation to ensure that an individual is aware only of the 'organisations' to which it usually discloses information of that kind. 'Organisation', however, has a restricted meaning for the purposes of the *Privacy Act*, excluding, for example, political parties and state or territory agencies. The OPC recommended in 2005 that the Australian Government consider amending NPP 1.3(d) to extend its coverage to disclosures generally, including to public sector agencies of the Australian Government, state or local governments, other bodies and private individuals.[152] The OPC stated that a narrow interpretation of this requirement seems inconsistent with the policy intent of the legislation, given that the Explanatory Memorandum envisaged disclosure to state government licensing authorities, which do not fall within the definition of 'organisation'.[153]

23.133 The OPC's guidance on the relevant obligation in the NPPs provides that:

> 'Reasonable steps' to inform an individual about the disclosures an organisation usually makes would ordinarily mean either giving general descriptions of sets of people and organisations (for example, 'State Government licensing authorities', 'health insurers' and 'list renters') or to list each member of the set.
>
> An organisation does not need to mention disclosures that the NPPs permit, but in practice happen only rarely. For example, it does not need to mention disclosures under warrant or to intelligence agencies.[154]

23.134 The OPC's guidance on the equivalent obligation in the IPPs provides that:

> Information is usually given to another party by an agency if the agency has a regular arrangement to give information to that party … [155]
>
> If possible, an agency should name each individual person or body to which it usually gives personal information. But if an agency can give information to a large number

---

151 See Ch 25.

152 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 74. Note, however, that the definition of 'organisation' extends to individuals.

153 See Ibid, 259; Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [3.34].

154 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 30.

155 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 18.

> of third parties, naming all of them could make the notice given to a person too long or unclear to be of help …
>
> *Suggestions*
>
> Agencies should generally name all federal organisations which they usually give personal information to.
>
> Generally, agencies should name other parties which they usually give personal information to. However, if an agency usually gives personal information to a group of organisations that do similar jobs (for example, State police forces), the agency can name the group rather than listing its individual members …
>
> If it is impractical to put the names of all the third parties that the agency gives information to on the form, the agency could give a leaflet with the form containing the IPP 2 notice.[156]

Submissions and consultations

23.135 In response to IP 31, one stakeholder supported expanding the obligation on organisations to ensure that individuals are aware of the disclosures made by organisations generally.[157] Another stakeholder suggested that, while agencies and organisations should be permitted to give generic descriptions of the entities to which they usually disclose personal information, they also should be required 'to answer any specific inquiries about whether a particular named agency or organisation is a recipient'.[158]

23.136 In DP 72, the ALRC proposed that, where agencies and organisations collect personal information from an individual either directly or from someone other than the individual, they should take reasonable steps to ensure that the individual is aware of the 'types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information'.[159]

23.137 Some stakeholders expressed concern that the obligation did not go 'far enough' because it required notification only of 'types' of entities to which the information is 'usually' disclosed.[160] For example, one stakeholder stated:

> This appears to readily allow various components of 'personal information' to be disclosed to another entity without notification because it is not 'usual' to disclose everyone's personal information to that particular entity.[161]

---

156 Ibid, 19.
157 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.
158 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.
159 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(f), 20–5(a)(i).
160 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; I Graham, *Submission PR 427*, 9 December 2007.
161 I Graham, *Submission PR 427*, 9 December 2007.

23.138 PIAC stated:

> While PIAC accepts that it would be impossible to identify every specific agency or entity to whom information may be released, a notification that it will be released to generic categories such as 'solicitors' or 'accountants' is likely to be of very limited use to an individual who is trying to decide whether or not to provide his or her personal information in the first place. In PIAC's view … data collectors should have to answer specific questions from the individual about the identity of actual recipients.[162]

23.139 Medicare Australia questioned the distinction between the current requirement on agencies to provide details of bodies or agencies in respect of which it is their usual practice to disclose personal information of the kind collected, and the proposed requirement which requires details of 'types' of bodies.[163]

23.140 Another stakeholder noted that the organisations to which personal information are usually disclosed is stated in a Privacy Policy. It expressed the view that to require a description of disclosures, specifically tailored to each collection of personal information, would be onerous and expensive.[164]

23.141 The ALRC also proposed that the OPC 'should provide guidance to assist agencies and organisations in ensuring that individuals are properly informed of the persons to whom their personal information is likely to be disclosed'.[165] This proposal was generally supported.[166] PIAC, while agreeing that guidance in this area is needed, expressed a preference for that guidance to be included in the *Privacy Act*, regulations or binding codes.[167] Another stakeholder expressed concern that guidance may require organisations to be more specific in the descriptions that they are to give.[168]

---

162 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. Another stakeholder expressed a similar view about answering specific inquiries: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

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

164 Confidential, *Submission PR 536*, 21 December 2007.

165 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 20–3.

166 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Federal Police, *Submission PR 545*, 24 December 2007; 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; 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; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 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.

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

168 Confidential, *Submission PR 536*, 21 December 2007.

ALRC's view

23.142 Agencies and organisations should be required to notify, or otherwise ensure that individuals are aware of the *actual* or *types* of agencies, organisations, or entities to which, or other persons to whom, agencies and organisations usually disclose personal information of the kind collected.

23.143 Agencies and organisations are currently subject to requirements to inform individuals of the actual entities to which they disclose personal information. The OPC's interpretation of this obligation as it applies to agencies and organisations, however, allows expressly for generic descriptions to be given in certain circumstances. NPP 1.3(d) also allows generic descriptions to be given. Framing the obligation in the manner recommended by the ALRC below more closely resembles the current position than that proposed in DP 72, and is therefore less likely to cause confusion in its application.

23.144 There are sound policy reasons for clarifying that the obligations of an organisation concerning notification of usual disclosures extends beyond disclosures to organisations. The obligations also encompass disclosures to agencies, state and territory bodies, individuals and other entities. First, this appears to reflect better the original intention of the provision. Secondly, it is unhelpful and unfair to individuals whose personal information is collected by organisations to be informed only of usual disclosures to other organisations. Presenting individuals with a complete picture of usual disclosures—as they are currently entitled to receive in relation to the collection of their personal information by agencies—allows them to make more informed decisions about withholding, or otherwise taking steps to protect, their personal information.

23.145 The specificity of the information required to comply with this requirement will depend on the circumstances. There is a need to strike a balance between providing useful and digestible information to an individual and ensuring that the costs and compliance burden in meeting the obligation are not unduly onerous.

23.146 The OPC should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. In particular, this guidance should address the appropriate level of specificity when notifying individuals about the entities to which personal information of the kind is usually disclosed.

Notification of avenues of complaint

23.147 Neither the IPPs nor NPPs require an agency or organisation to notify an individual, at the time of collection of personal information, of the avenues of complaint available to the individual if he or she has a privacy complaint. The OPC

Review recommended that the Australian Government consider amending the relevant obligation in the NPPs, in order to impose such an obligation on organisations.[169]

Submissions and consultations

23.148 In response to IP 31, stakeholders expressed strong support for requiring agencies and organisations to make individuals aware of the avenues of complaint available when personal information is collected.[170] In supporting such reform, the Australian Privacy Foundation stated that the principle should require notification of 'both internal and external dispute resolution options'.[171]

23.149 In DP 72, the ALRC proposed that, where agencies and organisations collect personal information from an individual, either directly or from someone other than the individual, they should take reasonable steps to ensure that the individual is aware of avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.[172]

23.150 The Office of the Victorian Privacy Commissioner expressed strong support for this proposal.[173] A number of stakeholders, however, expressed concerns about the level of detail in the 'Notification' principle and, in particular, the duplication of requirements in the proposed 'Notification' and 'Openness' principles.[174] They suggested that complaint management was relevant to general processes, and should be dealt with only in the 'Openness principle'.[175]

23.151 The ABA opposed such an approach, on the basis that banks already provide complaint handling and dispute resolution information under the *Corporations Act*, the

---

169 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 41.

170 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.

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

172 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposals 20–2(g), 20–5(a)(i).

173 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. It was also expressly supported by privacy advocates: Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

174 Confidential, *Submission PR 570*, 13 February 2008; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007.

175 Confidential, *Submission PR 570*, 13 February 2008; Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Government Department of Defence, *Submission PR 440*, 10 December 2007. Another stakeholder expressed the similar view that some of the detail in the proposed 'Notification' principle could be covered by the 'Openness' principle: Australian Government Centrelink, *Submission PR 555*, 21 December 2007.

Code of Banking Practice,[176] and the Electronic Funds Transfer Code of Conduct.[177] It stated that:

> If the proposed specific notification principle proceeds, then the compliance note at the end of the proposed principle should make reference to existing notification requirements under another law or code that reflect best practice and should be treated as capable of meeting the proposed requirement.
>
> This approach would also facilitate layered short form privacy information statements that supplement other information statements that banks are required to make under other laws.[178]

ALRC's view

23.152 There should not be unnecessary overlap between the requirements in the 'Notification' and 'Openness' principles. Duplicating requirements wastes resources and is likely to increase compliance costs—for example, increasing costs associated with publishing material in privacy notices and Privacy Policies. To the extent that information to be provided to individuals relates to an agency's or organisation's general processes for the handling of personal information, that information should be located in a Privacy Policy, pursuant to the requirements of the 'Openness' principle. This also will reduce any unnecessary detail in privacy notices, making such notices more meaningful for individuals whose personal information is collected.

23.153 It is important that, at or about the time that personal information is collected, persons are notified, or otherwise made aware, of the fact that there are avenues of complaint available to them, in the event that they have a privacy complaint. The provision of such information promotes accountability and transparency. It also assists in creating a regulatory environment in which individuals are aware that they may take steps to protect their personal information. The benefits attached to the provision of such information are therefore analogous to those relating to informing individuals about their rights of access to, and correction of, personal information.

23.154 It is unnecessary, however, for an individual to be provided with notification at the time of the collection of his or her personal information about the *actual* avenues of complaint available. This type of information is situated more appropriately in the Privacy Policy of an agency or organisation. The ALRC recommends, therefore, that at or about the time of collecting personal information, an agency or organisation should notify, or otherwise ensure that individuals are aware of, the fact that the avenues of complaint available to the individual are set out in the agency's or organisation's Privacy Policy.[179]

---

176 Australian Bankers' Association, *Code of Banking Practice* (1993).

177 Australian Securities and Investments Commission, *Electronic Funds Transfer Code of Conduct [amended March 2002]* (2001).

178 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008. These concerns are addressed in Ch 24.

179 This is discussed further in Ch 24.

Information required or authorised by or under law

23.155 Agencies are currently required, where applicable, to ensure that individuals are aware of the fact that a collection of information is authorised or required by or under law.[180] The OPC's guidance on this obligation provides that:

> An IPP 2 notice should refer to each provision of legislation which:
>
> - requires an agency to collect the personal information; or
> - specifically authorises an agency to collect the information.
>
> If legislation does not refer to a specific power, but only gives the agency a general function which includes collecting personal information, the IPP 2 notice should still refer to the legislation.[181]

23.156 Organisations are currently required to ensure that individuals are aware of 'any law that requires the particular information to be collected'.[182] The OPC's guidance on this obligation provides that:

> In describing the law the organisation need not specify the exact piece of legislation (although it would be desirable to do so where possible). A statement like 'taxation law requires us to collect this' would ordinarily be adequate.[183]

23.157 Stakeholders did not express concerns about the application of these requirements to agencies or organisations.

ALRC's view

23.158 An obligation relating to notification of personal information required or authorised by or under law should be retained and standardised for agencies and organisations. Standardising the obligation is consistent with creating a single set of privacy principles.[184]

23.159 The obligation imposed on agencies in the IPPs, on its face, is less onerous than the equivalent obligation imposed on organisations by the NPPs. The OPC's guidance, however, takes a stricter approach in the interpretation of the obligation as it applies to agencies.

23.160 The obligation is of particular relevance to the many agencies that have coercive information-gathering powers.[185] In recognition of this fact, from a practical perspective, it is appropriate to use the current IPP as the template for drafting this

---

180 *Privacy Act 1988* (Cth) s 14 , IPP 2(d).

181 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 17.

182 *Privacy Act 1988* (Cth) sch 3, NPP 1.3(e).

183 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 31.

184 See Ch 18.

185 See Australian Law Reform Commission, *Privilege in Perspective*, ALRC 107 (2008), ch 4 for an overview of federal bodies with coercive information-gathering powers.

particular obligation.[186] Agencies and organisations, therefore, should be required, where applicable, to notify, or otherwise ensure that an individual is aware of, the fact that the collection is required or authorised by or under law.

23.161 The OPC should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. This guidance should address, in particular, what is required of organisations in light of the recommended rewording of the obligation as it applies to them.

Source of information

23.162 Neither the NPPs or IPPs impose a requirement that an individual be notified of the source of personal information, where that information was provided by a third party.

23.163 There is some precedent for this requirement in other jurisdictions. For example, German law provides that a data subject should be provided with information about stored data concerning him or her, including any reference to the origin of the data.[187]

Submissions and consultations

23.164 In IP 31, the ALRC sought views about whether agencies and organisations should be obliged to inform individuals of the source of their personal information, where it is not collected directly from the individual.[188]

23.165 In response to IP 31, some stakeholders supported the imposition of such a requirement.[189] Others expressed reservations about such an approach. Stakeholders stated that, in some circumstances, it is necessary to protect the identity of the source.[190] They noted that revealing the source could place an individual at risk of domestic violence,[191] or otherwise present a serious threat to life or health.[192]

23.166 UNITED Medical Protection Ltd submitted that such a notification requirement is unnecessary because it 'will either occur as a matter of necessity or be obvious on its face'.[193]

---

186 As discussed in Ch 18, as a general proposition, the NPPs are to be preferred as a template for the drafting of the UPPs.

187 See *Federal Data Protection Act 1990* (Germany) ss 19(1), 34(1).

188 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.59].

189 See Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007; W Caelli, *Submission PR 99*, 15 January 2007.

190 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

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

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

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

23.167 In DP 72, the ALRC proposed that, where agencies and organisations collect personal information from someone other than the individual, they should take reasonable steps, on the request of the individual, to ensure that the individual is aware of the source of the information.[194]

23.168 Some stakeholders expressed strong opposition to the proposal. Organisations expressed the view that such a requirement would be unreasonable, impractical, highly onerous, unnecessary for data integrity purposes, and, in some circumstances, likely to interfere with the privacy of other individuals. They also said that it would impose excessive compliance costs while rendering marginal privacy protection to individuals.[195] Telstra, for example, noted that, in many cases, organisations would be unable to identify the source of the information but would have to 'expend significant time, cost and effort to endeavour to do so'.[196]

23.169 The ABA stated that such a requirement would duplicate disclosure to individuals made by the third parties that collected the personal information in the first place. Those third parties have obligations to ensure that an individual is aware of the entities to which the personal information is usually disclosed. The ABA stated:

> It seems an unnecessary compliance burden and cost to organisations that collect information from such third parties to in effect repeat the exercise upon request of the individual.[197]

23.170 The ABA also noted that systems would need to be put in place, regardless of whether the information about source was requested by an individual.

> The organisation must record the source of the information in all cases and secondly provide a telephone or other communication facility for the individual to make the request for the source of the information and for the organisation to comply with that request.
>
> This procedure would become even more complicated if the recipient organisation were required to provide details of the source of the information on request indefinitely.[198]

23.171 Agencies expressed concern about requiring such an obligation in the context of intelligence gathering, investigations and law enforcement. In particular, it was stated that such a requirement could: alert individuals that they are under investigation;[199] place witnesses at risk;[200] and breach the confidence between an

---

194 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 20–5(a)(ii).

195 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Confidential, *Submission PR 536*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007; Telstra Corporation Limited, *Submission PR 459*, 11 December 2007.

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

197 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

198 Ibid.

199 Confidential, *Submission PR 448*, 11 December 2007.

200 Confidential, *Submission PR 488*, 19 December 2007.

agency and a source who provided a confidential 'tip-off'.[201] Similar concerns were expressed about the application of such a requirement in the context of insurance fraud investigations.[202]

23.172 Others stated that, in some circumstances, disclosing the source of personal information would not be appropriate.[203] This would include circumstances where the requirement would interfere with the privacy of the individual who provided the information;[204] affect adversely the privacy of any other individual;[205] or pose a serious threat to the life or health of any individual.[206]

23.173 IFSA, for example, agreed with the proposal in principle, but stated that further consideration needs to be given to situations where information is collected on relatives, which is relevant to the assessment of insurance cover or the payment of superannuation death benefits to beneficiaries from insurance applicants and superannuation account holders. IFSA stated that:

> Life insurance and superannuation customers may not want family members or dependants to know that they are applying for insurance cover or nominating them as a beneficiary.
>
> Any requirement on companies to notify individuals that details have been supplied would impede the customer's right to their own privacy, particularly where the collection of information was incidental to the product or service offered.[207]

23.174 Agencies also expressed general concerns about the administrative burden and 'prohibitive' cost that would be imposed by all the requirements relating to notification in circumstances where an agency collects personal information from someone other than the individual, including the requirement relating to source.[208]

23.175 Some concern also was expressed about the scope of the requirement. The Law Council of Australia submitted that it should be made clear that 'source' in this

---

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

202 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.

203 Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007.

204 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

205 Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007. See also National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

206 One stakeholder submitted that such situations should be the subject of an exception to the requirement: National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 462*, 12 December 2007.

207 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007.

208 See, eg, Australian Government Department of Foreign Affairs and Trade, *Submission PR 563*, 24 January 2008; Australian Government Department of Families, Housing, Community Services and Indigenous Affairs, *Submission PR 559*, 15 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.

context referred to the entity from which the agency or organisation collected the information, rather than the ultimate source of the information.[209]

23.176 Some stakeholders supported this proposal unconditionally.[210] Privacy advocates supported the proposal but submitted that it should be made clear that the *identity* of the source of the information should be provided on request.[211]

ALRC's view

23.177 Imposing a general requirement on agencies and organisations to inform individuals, on request, of the source of personal information is potentially unworkable, costly and impractical. Such a requirement cannot be justified on a cost and benefit basis. Even if the requirement were limited to providing information on request, the reality is that agencies and organisations would have to set up systems to record the source of information in each case of indirect collection in order to comply with any such request. The sheer volume of transactions that agencies and organisations enter into every year, involving the indirect collection of personal information, would render the imposition of such a requirement excessive and burdensome.

23.178 Increasing the compliance burden could be justified, however, if it were likely to be outweighed by the benefits to be conferred on individuals by way of increased privacy protection. Arguably, informing individuals about the source of their personal information increases the control that they have over their personal information, and the likelihood that they will seek access to, and correct, it if necessary. This would promote the quality of personal information kept by agencies and organisations.

23.179 Other protections recommended by the ALRC, however, address the issue of data quality. In particular, under the 'Notification' principle, agencies and organisations have an obligation to notify or otherwise ensure that individuals are aware of: the fact of collection; and rights of access to, and correction of, personal information. Provision of this information, in itself, is likely to be sufficient to enable an individual to take steps to ensure the quality of personal information that has been collected from another source. Further, agencies and organisations are under an obligation to take reasonable steps to ensure that the personal information they collect—including from persons other than the individual concerned—is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-

---

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

210 Optus, *Submission PR 532*, 21 December 2007; Centre for Law and Genetics, *Submission PR 497*, 20 December 2007; Carers Australia, *Submission PR 423*, 7 December 2007. The Australian Direct Marketing Association stated that it 'did not disagree' with the proposal: Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007.

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

date and relevant.[212] Knowledge of the source of the information is therefore not essential to protect data quality.

23.180 Other recommendations made by the ALRC also would increase the level of control that an individual has over his or her personal information. As noted above, the ALRC has recommended that agencies and organisations should be required to notify individuals about usual disclosures to entities of personal information of the kind collected. Because one agency's or organisation's disclosure of personal information equates to another entity's collection of personal information, this requirement increases the likelihood that individuals also will be alerted to the potential sources of collection of their personal information.

23.181 While imposing a general requirement on agencies and organisations to notify individuals about the source of the information on request is, on balance, untenable, there is merit in imposing such a requirement in the direct marketing context. As discussed in Chapter 26, individuals who received unsolicited direct marketing communications were concerned about how the organisations in question obtained their details. The ALRC recommends that an organisation that direct markets to non-existing customers or to persons under the age of 15 must, if requested by the individual, and it is reasonable and practicable to do so, advise the individual of the source from which it acquired the individual's personal information.[213]

23.182 In light of the above-mentioned recommendations, in the ALRC's view, the imposition of a general requirement to notify individuals of source of personal information, upon request, is unlikely to deliver any meaningful additional privacy protection to individuals.

Recommendation 23–2 The 'Notification' principle should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify or otherwise ensure that the individual is aware of the:

(a) fact and circumstances of collection where the individual may not be aware that his or her personal information has been collected;

(b) identity and contact details of the agency or organisation;

(c) rights of access to, and correction of, personal information provided by these principles;

212 The 'Data Quality' principle is discussed in Ch 27.
213 See Ch 26.

(d) purposes for which the information has been collected;

(e) main consequences of not providing the information;

(f) actual, or types of, agencies, organisations, entities or persons to whom the agency or organisation usually discloses personal information of the kind collected;

(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and

(h) fact, where applicable, that the collection is required or authorised by or under law.

Recommendation 23–3 The Office of the Privacy Commissioner should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. In particular, the guidance should address:

(a) the circumstances when it would and would not be reasonable for an agency or organisation to take no steps to notify individuals about the matters specified in the 'Notification' principle. In this regard, the guidance should address the circumstances when:

  (i) notification would prejudice the purpose of collection, for example, where it would prejudice:

    - the prevention, detection, investigation, and prosecution of offences, breaches of law imposing a penalty or seriously improper conduct;

    - the enforcement of laws; or

    - the protection of the public revenue;

  (ii) the collection of personal information is required or authorised by or under law for statistical or research purposes;

  (iii) the personal information is collected from an individual on repeated occasions;

  (iv) an individual has been made aware of the relevant matters by the agency or organisation which disclosed the information to the collecting agency or organisation;

(v) non-compliance with the principle is authorised by the individual concerned;

(vi) the taking of no steps is required or authorised by or under law;

(vii) notification would pose a serious threat to the life or health of any individual; and

(viii) health services collect family, social or medical histories;

(b) the appropriate level of specificity when notifying individuals about anticipated disclosures to agencies, organisations, entities and persons; and

(c) the circumstances in which an agency or organisation can comply with specific limbs of the 'Notification' principle by alerting an individual to specific sections of its Privacy Policy or to other general documents.

Summary of 'Notification' principle

23.183 The third principle in the model UPPs should be called 'Notification'. It may be summarised as follows.

UPP 3. Notification

At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

(a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;

(b) identity and contact details of the agency or organisation;

(c) rights of access to, and correction of, personal information provided by these principles;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;

(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and

(h) fact, where applicable, that the collection is required or authorised by or under law.

24. Openness

Contents

Introduction

24.1 Openness requires that the personal information-handling practices of agencies and organisations are transparent. This chapter considers whether requirements relating to openness should be contained in a discrete privacy principle. It recommends that Privacy Policies should be the mechanism by which openness is achieved. It considers: what should be included in Privacy Policies; how they should be made available; and should they be supplemented by short form privacy notices.

Current coverage by IPPs and NPPs

24.2 The Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) both set out openness requirements. IPP 5.1 provides that a record-keeper, in possession or control of records containing personal information, must take such steps as are reasonable in the circumstances to enable any person to ascertain:

- whether the record-keeper has possession or control of any records that contain personal information; and, if so

- the nature of the information, the main purposes for which it is used and how to gain access to the record containing the information.

24.3 The record-keeper does not need to comply with IPP 5.1 if required or authorised to refuse to give that information by a federal law that provides for access to documents.[1] A record-keeper is also required to maintain a record setting out: the nature of the records of personal information it keeps; 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; who is entitled to access the personal information, and upon what conditions; and how persons can access the information. The record-keeper is to make the record setting out the above information available for public inspection, and is to give the Privacy Commissioner a copy of the record in June each year.[2]

24.4 NPP 5 provides that an organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it. On request, an organisation must take reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

A separate 'Openness' principle

24.5 The ALRC has considered whether the requirements relating to openness should continue to be dealt with in a discrete privacy principle. As noted in Chapter 23, in response to the Issues Paper, *Review of Privacy* (IP 31), some stakeholders expressed the view that the notification and openness requirements should be located within the same principle.[3] Specifically, some stakeholders suggested an 'awareness principle', which would cover 'notification requirements at the time of collection and more general information provision'.[4] It was stated that attention should be given to the respective roles of proactive notice and obligations to respond to inquiries.[5]

---

1 The two main pieces of federal legislation providing for access to documents are the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth). Access to personal information is dealt with in Ch 29.

2 This is discussed further in Part F of this Report.

3 See, eg, 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.

4 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.

5 Ibid.

24.6 In the Discussion Paper, *Review of Australian Privacy Law* (DP 72), the ALRC proposed that the model Unified Privacy Principles (UPPs) should contain a discrete principle called 'Openness' that sets out the requirements on agencies or organisations to operate openly and transparently by providing general information on how they collect, hold, use and disclose personal information.[6]

24.7 This proposal generally was supported.[7] For example, Privacy NSW expressed the view that an openness principle would not only 'increase the transparency of organisations' and agencies' dealings with regard to … personal information', but would also 'assist in identifying and remedying compliance issues'. It also expressed the view that the principle should be entitled 'Privacy Policy' in order to distinguish it from the 'Notification' principle.[8]

24.8 The Public Interest Advocacy Centre (PIAC) stated that the ALRC's approach would consolidate and simplify the existing requirements, and that:

> A separate UPP dealing with 'Openness' will also serve to highlight the importance of this principle as a mechanism for ensuring open and transparent handling of personal information by agencies and organisations.[9]

ALRC's view

24.9 The requirements on an agency or organisation to operate openly and transparently by providing general information on how it manages personal information should be dealt with in a discrete principle in the model UPPs.

24.10 It is not appropriate to deal with requirements relating to openness and notification in the same principle because of their important conceptual differences. Openness provisions require agencies and organisations to make their general practices relating to the handling of personal information transparent. The requirement is not targeted exclusively for the benefit of those whose personal information has been, or is

---

6 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 21–1.

7 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 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; 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; Australian Unity Group, *Submission PR 381,* 6 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353,* 30 November 2007. The Australian Direct Market Association stated that 'it did not disagree' with the proposal: Australian Direct Marketing Association, *Submission PR 543,* 21 December 2007.

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

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

to be, collected. The obligation attaches regardless of whether an agency or organisation has actually collected personal information from a particular individual, or plans to do so.

24.11 In contrast, the requirement to notify or otherwise ensure an individual is aware of specified matters under the 'Notification' principle applies *only* when an individual's personal information has been, or is to be, collected. Further, the 'Notification' principle is directed to informing the particular individual how the agency or organisation will, or is likely to, handle his or her personal information, or personal information *of the kind* collected from the individual.

24.12 The benefits that flow from compliance with the openness requirements therefore can be distinguished in their nature and scope from those relating to notification. The publication of explanations as to how agencies and organisations deal with personal information generally benefits the regulatory system as a whole. It allows, for example, the Office of the Privacy Commissioner (OPC) to monitor an agency's or organisation's compliance with the *Privacy Act* and also to recommend changes to the personal information management practices of the agency or organisation.[10] Openness, therefore, plays a key role in promoting best practice in the handling of personal information.

24.13 It is preferable for the principle to be given a name which reflects its goal—that is, 'openness'—rather than one that describes the regulatory mechanism by which that goal is to be achieved—such as 'Privacy Policy'. This approach better reflects the high-level nature of the privacy principles.

Regulatory mechanism: 'Privacy Policies'

24.14 The IPPs and NPPs set out different regulatory mechanisms by which openness is to be achieved. Currently, agencies are required to:

- take such steps as are, in the circumstances, reasonable to enable any person to ascertain specified matters;[11]
- maintain a record setting out a number of matters relating to the agency's handling of personal information;[12] and
- make the record available for inspection by the public and give a copy annually to the OPC, which uses this to create the Personal Information Digest.[13]

---

10 This is discussed in greater detail in Part F.

11 See *Privacy Act 1988* (Cth) s 14, IPP 5.1.

12 See Ibid s 14, IPP 5.3.

13 See Ibid s 14, IPP 5.4. See also s 27(1)(g). In New South Wales, agencies are required to prepare privacy management plans, which describe the agency's policies and practices to ensure compliance with privacy legislation. These plans are to be provided to the Privacy Commission after preparation and whenever amended: See *Privacy and Personal Information Protection Act 1998* (NSW) s 33.

24.15 Organisations are required to:

- produce a document, available to anyone on request, which sets out the organisation's policies on its management of personal information; and

- take reasonable steps, on request, to inform a person generally about: what sort of personal information it holds; for what purposes; and how it collects, holds, uses and discloses that information.[14]

Submissions and consultations

24.16 In response to IP 31, strong concern was expressed that the Personal Information Digest mechanism applicable to agencies is not operating effectively.[15] Some stakeholders suggested that the Personal Information Digest is of limited utility and the information could be disseminated better in other ways.[16] For example, AAMI stated that requiring organisations to submit their documents annually to the OPC 'would be unlikely to add any real value'.[17] The Australian Federal Police suggested that such information could be made available 'through self publishing on agency websites in line with guidelines issued by the Privacy Commissioner'.[18]

24.17 In DP 72, the ALRC proposed that the 'Openness' principle should set out the requirements on an agency or organisation to operate openly and transparently by providing general notification in a Privacy Policy of how it manages, collects, holds, uses and discloses personal information.[19]

24.18 This proposal received general support.[20] For example, Medicare Australia expressed the view that the Privacy Policy mechanism 'would provide clear detail for both the agency and the individual' and is 'much more useful than the current [Personal Information Digest arrangements] under IPP 5'.

---

14 See *Privacy Act 1988* (Cth) sch 3, NPP 5.

15 The concerns about the Personal Information Digest system are described in detail in Ch 47.

16 See Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

17 AAMI, *Submission PR 147*, 29 January 2007.

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

19 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 21–1.

20 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 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; 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; Australian Unity Group, *Submission PR 381*, 6 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

24.19 The Australian Privacy Foundation stated that, although 'there has been relatively little use' of the Personal Information Digest, it remains a 'potentially valuable resource for the media and public interest groups to make comparisons and hold governments to account'. It therefore supported a requirement for an agency to provide to the Privacy Commissioner an electronic copy of its Privacy Policy at least once a year.[21]

24.20 PIAC made the point that, in order to be effective, a policy must be implemented. It submitted that the 'Openness' principle should make it clear that agencies and organisations should take reasonable steps to implement their Privacy Policies.[22]

ALRC's view

24.21 The openness requirements, currently located in the IPPs and NPPs, should be consolidated and simplified in the model UPPs. The 'Openness' principle should make it clear that a Privacy Policy is the regulatory mechanism by which agencies and organisations are to achieve openness. Agencies and organisations should be required to set out in Privacy Policies clearly expressed policies on their handling of personal information.[23]

24.22 The development of Privacy Policies will have a positive impact on the regulatory system as a whole. It will assist in the OPC's auditing process,[24] and in promoting best practice in the handling of personal information. By requiring agencies and organisations to express in their Privacy Policies how they handle personal information at each stage of the information cycle, agencies and organisations will be encouraged to consider how the UPPs apply to their activities. This may assist agencies and organisations to structure their operations so as to comply with the UPPs.

24.23 The development and publication of Privacy Policies will promote the accountability of agencies and organisations. If agencies and organisations do not adhere to their Privacy Policies, the policies expressed in such documents may be used as a benchmark against which actual practices relating to the handling of personal information may be judged.

24.24 Privacy Policies also will increase the transparency of the information-handling practices of particular agencies and organisations. This will allow individuals to make more informed choices about whether they wish to transact with particular agencies or organisations.

---

21 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008.
22 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
23 The content and availability of Privacy Policies are addressed below.
24 The OPC's audit function is discussed in Part F.

24.25 Agencies should not be required to submit their Privacy Policies to the OPC each year for the purposes of the Personal Information Digest.[25] The posting of Privacy Policies on the websites of agencies, and the requirement that such policies be made available in hard copy, on request, makes it unnecessary for agencies to submit their Privacy Policies to the OPC for the purpose of the 'Openness' principle.[26] The removal of this requirement will ease the compliance burden on agencies.

24.26 It is important that agencies and organisations implement their Privacy Policies. Staff should be trained to ensure that they are aware of the contents of Privacy Policies, and the obligations that ensue.

Content of a Privacy Policy

24.27 The openness requirements applicable to agencies and organisations differ. NPP 5 imposes a general obligation on an organisation to maintain a document setting out 'clearly expressed policies on its management of personal information', whereas IPP 5 takes a more prescriptive approach. As noted above, IPP 5 lists the specific matters that must be included in the record summarising how the agency handles personal information. These matters are: the nature of the records of personal information it keeps; 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; who is entitled to access the personal information, and upon what conditions; and how persons can access the information.

24.28 In addition to the maintenance of some kind of document setting out their personal information-handling practices, the openness provisions under the IPPs and NPPs impose requirements on agencies and organisations to take reasonable steps to ensure openness. Under IPP 5, agencies are required to take such steps as are reasonable in the circumstances to enable any person to ascertain:

- whether the agency has possession or control of any records that contain personal information; and,
- if so the: nature of the information; main purposes for which it is used; and the steps to be taken to obtain access to the record.

24.29 Under NPP 5, an organisation is required on request by a person, to take reasonable steps to let that person know generally about: what sort of personal information it holds; for what purposes it holds that information; and how it collects, holds, uses and discloses that information.

---

25 This is discussed in Ch 47.

26 The availability of Privacy Policies is discussed below.

24.30 There are some requirements relating to content that are common to the IPPs and NPPs, therefore, even though the stipulated regulatory mechanisms for delivering that information content differ for specific matters. That is, both sets of privacy principles require disclosure of the sort of personal information that is held, and the purposes for which personal information is held.

Submissions and consultations

24.31 In response to IP 31, some stakeholders supported the imposition of more prescriptive openness requirements on organisations. For example, it was submitted that organisations should make available the 'details of the information systems used to maintain relevant databases' because this would allow individuals to assess the security and other qualities of the information-handling system.[27] Another stakeholder stated that the OPC should be given the discretion to 'require organisations to publish further information about particular personal information handling projects'.[28]

24.32 The OPC submitted that 'the obligations imposed by NPP 5 require more specificity to remain relevant and effective', but this should not allow the principle to become too prescriptive. In the OPC's view, this would run contrary to the regulatory framework of the Act.[29] Some stakeholders also noted that greater guidance could be provided in guidelines, as distinct from primary legislation.[30]

24.33 Other stakeholders opposed taking a prescriptive approach to the openness obligations.[31] They stated that a prescriptive approach would hamper the ability of organisations to tailor privacy policies to customers' needs and it may lead to lengthy and complex privacy policies.[32]

24.34 In DP 72, the ALRC proposed that agencies and organisations should be required to set out in a Privacy Policy their policies on the management of personal information, including how personal information is collected, held, used and disclosed. The ALRC proposed that this document should also include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

---

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

28 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.

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

30 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

31 Law Council of Australia, *Submission PR 177*, 8 February 2007; Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

32 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007.

(c) the avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) the steps individuals may take to gain access to personal information about them held by the agency or organisation;

(e) the types of individuals about whom records are kept;

(f) the period for which each type of record is kept; and

(g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.[33]

General responses

24.35 Some stakeholders supported this proposal.[34] For example, the Office of the Victorian Privacy Commissioner (OVPC) stated that:

> There is benefit in a slightly more prescriptive approach towards 'Openness', provided that the additional details required by (a) to (g) do not require an agency or organisation to provide an exhaustive list of those matters, but rather a general one …
>
> The additional details proposed in (a) to (g) would provide an organisation with a better guide as to how to meet this aspect of an openness principle and enhance the general public's understanding about personal information that is held by organisations and the organisations' resulting obligations.[35]

24.36 The OPC agreed in principle with the proposal, but noted 'it may be somewhat more prescriptive than required and hence may be contrary to the intention of having high-level principles in the *Privacy Act'*. It stated that the proposed approach would 'pose the risk that the prescribed matters might be taken as an exhaustive list of factors for an openness policy'.[36]

24.37 The OPC expressed the view that the matters to be stated in the 'Openness' principle for inclusion in a Privacy Policy should be limited to: the sort of personal information held; the purposes for which it is held; and the steps individuals may take to gain access.[37] Another stakeholder expressed a similar view on the essential content

---

33 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 21–2.

34 Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the 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; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

35 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007. Optus also expressed support on the basis that it was made clear that the descriptions to be given could be high-level, rather than detailed: Optus, *Submission PR 532*, 21 December 2007.

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

37 Ibid. The OPC also stated that, where necessary, it would issue guidance on the content of an agency's or organisation's policies on the management of personal information.

of a Privacy Policy, but stated that the avenues of complaint available to an individual should also be included.[38]

24.38 PIAC stated that Privacy Policies also should refer to the fact that an individual can seek to correct his or her personal information.[39]

24.39 Other stakeholders expressed opposition to the ALRC's proposal,[40] or to specific limbs of the proposal.[41] Reasons for opposing the proposal included that:

- it is overly prescriptive;[42]
- a 'one size fits all' approach is inappropriate because it fails to recognise: the competitive nature of organisations as opposed to agencies; and that organisations have different business imperatives and customer relationships;[43]
- some of the information proposed to be included in Privacy Policies is already included in other customer documents—such as Product Disclosure Statements;[44]
- it would result in lengthy, detailed and complex Privacy Policies, which is likely to discourage individuals from reading them;[45] and
- it would impose significant compliance costs on organisations.[46]

24.40 One stakeholder opposed the inclusion of all of the matters proposed to be included in a Privacy Policy, other than information about avenues of complaint and the steps individuals can take to seek access to their personal information. It stated that the requirements objected to:

- 'serve little or no constructive purpose because most people do not have the time or sufficient interest in these details';

---

38 Confidential, *Submission PR 570*, 13 February 2008.
39 Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.
40 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007. See also Confidential, *Submission PR 570*, 13 February 2008; Law Council of Australia, *Submission PR 527*, 21 December 2007.
41 Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Confidential, *Submission PR 536*, 21 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007. Responses to specific limbs of the proposal are addressed separately below.
42 Confidential, *Submission PR 570*, 13 February 2008.
43 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.
44 Suncorp-Metway Ltd, *Submission PR 525*, 21 December 2007.
45 Confidential, *Submission PR 536*, 21 December 2007; Law Council of Australia, *Submission PR 527*, 21 December 2007.
46 Confidential, *Submission PR 536*, 21 December 2007.

- are inappropriate for the private sector; and
- will be difficult and costly to comply with, particularly on an ongoing basis.[47]

24.41 The Law Council of Australia noted that organisations currently focus on their core customer base in Privacy Policies. It stated that:

> If [the proposal] were adopted then it would be very clear that the Privacy Policy needed to address not only customers but also applicants for employment, employees (if the employee record exemption is removed), individuals who work for the organisation's suppliers and service providers, other business contacts etc. For some of these categories of individual (in particular business contacts and employees of suppliers and service providers) the information held is typically only basic business contact information. The Law Council questions the value of addressing each of paragraphs (a) to (d), (f) and (g) in relation to that type of personal information, particularly if to do so materially adds to the length and complexity of the Privacy Policy.[48]

24.42 Another stakeholder expressed general concern that there not be overlap between the requirements of a Privacy Policy and those relating to notification.[49]

Types of individuals about whom records are kept

24.43 Some stakeholders opposed the mandatory inclusion in a Privacy Policy of a description of the types of individuals about whom records are kept.[50] For example, one stakeholder stated that such a requirement is unnecessary because the types of people about whom information is kept 'is usually directly connected to the purpose(s) for which personal information is collected, used and disclosed'.[51]

Retention period

24.44 Many stakeholders expressed opposition to the proposed requirement that organisations be required to set out in a Privacy Policy the period of time for which each type of record is kept.[52] They stated that such a requirement is impracticable and costly, particularly in the financial services industry. This was said to be due to the

---

47 Ibid.

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

49 GE Money Australia, *Submission PR 537*, 21 December 2007. Concerns about the duplication of requirements in the 'Openness' and 'Notification' principles also are discussed in Ch 23.

50 Confidential, *Submission PR 570*, 13 February 2008; Confidential, *Submission PR 536*, 21 December 2007.

51 Confidential, *Submission PR 570*, 13 February 2008.

52 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008; Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; 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; Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

number of different records that financial institutions hold, and the different retention requirements that exist in various statutes. For example, the Australian Bankers' Association stated that 'to devise an openness policy specifying the various retention periods would be a sizeable task and questionable on a cost and benefit analysis'.[53] Stakeholders also expressed the view that providing such information to customers would be unhelpful and confusing.[54]

24.45 Australian Unity Ltd opposed the particularisation of various periods of retention, noting that retention periods can depend on a variety of circumstances, such as whether a transaction is complete, or if litigation is pending. It supported, however,

> a generalised notification within the [organisation's] privacy policy stating records are maintained for a period consistent with applicable laws but no longer than a stated maximum period set by the organisation after consideration of the relevant laws directly affecting that industry.[55]

Guidance

24.46 In DP 72, the ALRC proposed that the OPC issue guidance on how agencies and organisations can comply with their obligations under the 'Openness' principle to produce and make available a Privacy Policy.[56]

24.47 This proposal was generally supported.[57] PIAC stated that the OPC also should provide guidance on the implementation of Privacy Policies. It stressed the importance of the OPC conducting audits of Privacy Policies to ensure compliance with the 'Openness' principle.[58]

ALRC's view

24.48 The 'Openness' principle should be less prescriptive than the one proposed in DP 72. It is necessary to strike an appropriate balance between the detail in the 'Notification' and 'Openness' principles. An assessment of the content of one principle cannot be made without reference to the other.

---

53 Australian Bankers' Association Inc, *Submission PR 567*, 11 February 2008.

54 For eg, Investment and Financial Services Association, *Submission PR 538*, 21 December 2007; Insurance Council of Australia, *Submission PR 485*, 18 December 2007.

55 Australian Unity Group, *Submission PR 381*, 6 December 2007.

56 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 21–3.

57 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; 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; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007.

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

24.49 The 'Notification' principle is relatively prescriptive. There is a strong argument that the 'Openness' principle, therefore, should be less prescriptive. This is consistent with the approach in the NPPs—the notification provisions of the collection principle are prescriptive, whereas the openness principle is expressed in high-level terms. Conversely, in the IPPs, the openness principle is prescriptive, and the notification provisions within the collection principle are comparatively less prescriptive.

Matters to be included

24.50 The essential content of a Privacy Policy should be expressed in high-level terms. That is, the central obligation should be for agencies and organisations to set out in such a document clearly expressed policies on an agency's or organisation's handling of personal information, including how it collects, holds, uses and discloses personal information. Any other matters required to be included in Privacy Policies, therefore, should not be interpreted as being exhaustive. The listing of such matters in the 'Openness' principle, however, should be limited, consistent with a less prescriptive approach. Such matters should include the sort of personal information the agency or organisation holds, and the purposes for which it is held. Both of these requirements are currently the subject of the IPPs and NPPs, so their inclusion in the 'Openness' principle should not add significantly to compliance costs.

24.51 Privacy Policies also should include the steps individuals may take to access and correct personal information. This information complements, but does not duplicate, a particular requirement under the 'Notification' principle. That is, that an agency or organisation is to notify or otherwise ensure that an individual whose personal information has been, or is to be, collected is aware of his or her rights under the UPPs to seek access to, and correction of, personal information. One obligation concerns notification of the right; the other, the process by which that right can be exercised. It is appropriate that information about general processes concerning personal information is the subject of the 'Openness' principle.

24.52 Similarly, Privacy Policies also should address the avenues of complaint available to individuals in the event that they have a privacy complaint. Significantly, the requirement is merely explanatory of the existing options available to individuals who may have a complaint. It does not require any new avenues of complaint to be made available. Again, this requirement complements, but does not duplicate, the requirement in the 'Notification' principle that individuals be made aware of the *fact* that the avenues of complaint available to them are set out in the agency's or organisation's Privacy Policy.

24.53 Ideally, information about avenues of complaint should include an internal dispute resolution contact and whether the agency or organisation is part of an external

dispute resolution scheme (such as the Telecommunications Industry Ombudsman or Banking and Financial Services Ombudsman).[59] The need for such details, however, should be addressed in OPC guidance, rather than being incorporated in the 'Openness' principle itself.

24.54 It is not necessary to duplicate the requirements imposed on organisations by different legislative and regulatory regimes. As noted in Chapter 23, banks are required under the *Corporations Act*, the Code of Banking Practice, and the Electronic Funds Transfer Code of Conduct to provide complaint handling and dispute resolution information. It should be sufficient, therefore, for a Privacy Policy to state, where applicable, that the avenues of complaint available to an individual are set out in another generally available document that has been prepared to comply with other legislative or industry requirements.

24.55 For the reasons discussed in Chapter 31, the Privacy Policy of an agency or organisation also should set out whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.[60]

Matters not required to be included

24.56 Agencies and organisations may choose, but should not be required, to include the following matters in their Privacy Policies:

- details of the types of individuals about whom records are kept;
- details of the persons, other than the individual, who can access personal information, and the conditions upon which they access it; and
- the period for which each type of record is kept.

24.57 Arguably, the types of individuals about whom records are kept. can be surmised from the purposes for which personal information is collected, used and disclosed. Similarly, information about persons, other than the individual, who can access personal information, should be apparent from:

- a general description of an agency's or organisation's disclosure practices in its Privacy Policy, including information about cross-border transfers; and

---

59 A similar obligation, in relation to internal dispute resolution, is provided for in the *Privacy and Personal Information Protection Act 1998* (NSW) s 33(2)(c).

60 See Rec 31–8.

- information provided about an agency's or organisation's usual disclosures of personal information of the kind collected, pursuant to the obligation in the 'Notification' principle.[61]

24.58 It may be costly and burdensome for some organisations, for example, those in the financial sector, to set out in their Privacy Policies, an explanation of the period of time for which they keep each type of record containing personal information. In particular, a statutory obligation in the *Privacy Act* to set out statutory retention periods contained in other legislation is an unnecessary compliance burden.

Alternative approach

24.59 The ALRC considered an alternative approach to reform of the 'Openness' principle. Most of the concerns expressed about the proposed matters to be included in a Privacy Policy related to their application to organisations. The alternative is to:

- restrict the specific matters that the 'Openness' principle should require for inclusion in an organisation's Privacy Policy to the: sort of information held; purposes for which it is held; steps that may be taken to access and correct personal information; and avenues of complaint; and

- provide that the 'Openness' principle should provide for more matters to be included in an agency's Privacy Policy. These should be the four matters mentioned above, as well as the matters in respect of which agencies currently have to provide details. That is, the Privacy Policies of agencies also should address: the types of individuals about whom records are kept; the period for which each type of record is kept; and the persons, other than the individual, who can access personal information and the conditions under which they can access it.

24.60 On balance, it would be simpler to have the same 'Openness' principle apply to both agencies and organisations to avoid the types of complications that currently arise due to the existence of a dual set of principles.[62] It should be emphasised, however, that the central obligation in the 'Openness' principle is for agencies and organisations to set out clearly expressed policies in their Privacy Policies about the management of personal information. Pursuant to such an obligation, agencies may still deem it appropriate to include information in their Privacy Policies about the specific matters that they currently are obliged to address.

---

61 See Ch 23; UPP 3(f).

62 Such complications are discussed in Ch 18.

Guidance

24.61 The ALRC anticipates that the OPC will develop and publish general guidance to assist agencies and organisations to comply with the 'Openness' principle. The ALRC notes the OPC's 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 24–1 The model Unified Privacy Principles should contain a principle called 'Openness'. The principle should set out the requirements on an agency or organisation to operate openly and transparently by setting out clearly expressed policies on its handling of personal information in a Privacy Policy, including how it collects, holds, uses and discloses personal information. This document also should include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the steps individuals may take to access and correct personal information about them held by the agency or organisation; and

(d) the avenues of complaint available to individuals in the event that they have a privacy complaint.

Availability of Privacy Policy

24.62 The NPPs and IPPs differ in that IPP 5 requires a record-keeper to take reasonable steps to enable an individual to ascertain specified matters regardless of whether the individual has made a request, whereas the corresponding obligation in NPP 5 only applies to an organisation following a request by an individual.

Submissions and consultations

24.63 In response to IP 31, some stakeholders submitted that the requirements to make certain information available should apply regardless of whether an individual has requested that information.[63]

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

24.64 Other stakeholders suggested that an individual's request should be the appropriate trigger for the provision of some types of information. AAMI, for example, submitted that:

> Disclosure regarding an organisation's privacy processes/procedures should only be required upon request. However, the consumer needs to be informed via short notices that they can request or amend their personal information if they so wish.[64]

24.65 The OVPC stated that:

> It is often administratively convenient for organisations to make their information-handling policies readily available (eg on the internet or in a brochure) without awaiting an individual request.
>
> The request mechanism is useful to enable individuals to obtain further information about matters that have not been addressed in the organisation's generic policy.[65]

24.66 The Australian Bankers' Association expressed concern about the amount of information that already must be made available to consumers. It stated that, if the obligations were triggered without an individual's request, customers could be over-burdened with 'paper information'.[66] The Australian Government Department of Health and Ageing also favoured extending the request-based approach in the NPPs to agencies, stating that this would be more cost effective and practically useful for individuals.[67]

24.67 In DP 72, the ALRC proposed that an agency or organisation should be required to take reasonable steps to make its Privacy Policy available without charge to an individual electronically (for example, on its website, if it possesses one); and in hard copy, on request.[68]

---

64 AAMI, *Submission PR 147*, 29 January 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007.

65 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

66 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007. See also National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007.

67 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

68 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 21–4.

24.68 Stakeholders generally supported this proposal.[69] Medicare Australia, for example, stated that this approach 'would meet the needs of [individuals] without adding an additional burden on agency resources'.[70] The OVPC stated that:

> To heighten awareness in information handling, there seems no reason why the obligation for an organisation to make its privacy policy available should be dependent upon first being asked by a member of the general public to produce it. However, this should not preclude an organisation from having to provide more detailed information about its handling practices than is generally stated in the privacy policy if requested.[71]

24.69 The OPC stated that:

> Attention should be paid to whether privacy policies are provided in a form that is accessible to individuals from non-English speaking backgrounds, and individuals with other special needs, such as the visually impaired. Agencies and organisations should consider such matters in light of their customer or constituent base.[72]

24.70 PIAC expressed a similar view, noting also the special needs of those who are illiterate, or unable to access a computer because of financial disadvantage. It suggested that, in circumstances where an individual is unable to access a Privacy Policy electronically or in hard copy, the policy should be made available in such other form as the individual requests.[73]

ALRC's view

24.71 Agencies and organisations should take reasonable steps to make their Privacy Policies available electronically—for example, on their websites, if they have one. The posting of Privacy Policies on websites is an ideal mechanism for making them generally available. This is consistent with the aims of the 'Openness' principle, namely increasing transparency and openness in the personal information-handling practices of agencies and organisations.

---

69 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; Medicare Australia, *Submission PR 534*, 21 December 2007; Optus, *Submission PR 532*, 21 December 2007; Confidential, *Submission PR 519*, 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; Australian Unity Group, *Submission PR 381*, 6 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. One stakeholder stated that such an obligation, however, should not apply to 'vexations or frivolous' requests: Optus, *Submission PR 532*, 21 December 2007.

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

71 Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007.

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

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

24.72 Agencies and organisations should be required to provide individuals with a hard copy of their Privacy Policies only on request. To mandate the provision of hard copies in the absence of a request would impose a significant compliance burden. It also would be of limited utility to individuals, especially those who have no dealings with a particular agency or organisation. Moreover, it may lead to individuals being overloaded with information in paper form, especially given that they already receive a large amount of general disclosure information in their transactions with government and the private sector. Finally, it is environmentally irresponsible.

24.73 Agencies and organisations also should take reasonable steps to make their Privacy Policies available in a form accessible to individuals with special needs, where this is requested. This would involve taking reasonable steps to ensure, for example, that individuals who are visually impaired, or from a non-English speaking background, can access Privacy Policies if they request to do so. The qualification that an agency or organisation need only take reasonable steps is significant. It allows for the possibility that meeting a particular request may not be reasonable. This may arise, for example, where the steps requested to be taken would impose an excessively disproportionate compliance burden compared with the privacy benefit likely to be gained by the individual making the request.

24.74 If an individual requests a copy of an agency's or organisation's Privacy Policy—whether in hard copy or in an alternative accessible form—he or she should not be charged a fee for this information. This reflects the underlying principle that an individual should not be unreasonably disadvantaged for seeking to assert or enjoy his or her privacy rights. This no disadvantage principle is discussed in Chapter 32.

Recommendation 24–2 An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the 'Openness' principle, available without charge to an individual electronically; and, on request, in hard copy or in an alternative form accessible to individuals with special needs.

Short form privacy notices

Background

24.75 A short form privacy notice is a summary of an agency's or organisation's practices for the management of personal information. By creating a short form privacy notice, an agency or organisation will not necessarily fulfil its obligations under the openness principle. Such a notice can be useful, however, in assisting individuals to understand quickly, in broad terms, how a particular agency or organisation handles personal information.

24.76 The obligation in NPP 5.1 for an organisation to maintain a document setting out its policies on the management of personal information has been described as 'somewhat vague about what it requires organisations to do'.[74] There is a question whether the requirement should make clear that short form privacy notices are included.

24.77 The OPC's review of the private sector provisions of the *Privacy Act* recommended that the Australian Government consider amending NPP 5.1 to provide for short form privacy notices. It said that this also could clarify the obligations on organisations to provide notice and clarify the links between NPP 1.3 (notification under the collection principle) and NPP 5.1 (openness).[75] The OPC said that short form notices 'would improve the quality of an organisation's communication with its customers' and, further:

> A long privacy notice may not fulfil its purpose of informing a consumer because the consumer may be overwhelmed and confused … The Office's Community Attitudes Survey reports international research that shows that people do not necessarily read privacy notices, partly because they are too long and complex.[76]

24.78 The OPC stated that it would encourage the development of short form privacy notices. It would play a more active role in assisting businesses develop their notices by 'developing template notices for different sectors, in consultation with them, and by issuing examples of both satisfactory and unsatisfactory notices'.[77]

Submissions and consultations

24.79 In response to IP 31, many stakeholders supported the privacy principles making provision for short form privacy notices.[78] Some stakeholders noted that they already provide short form privacy notices.[79]

24.80 The OPC stated that :

> Short form privacy notices are an important aspect of assisting the individual to be meaningfully informed.

---

74 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 91.

75 Ibid, rec 19.

76 Ibid, 91–92.

77 Ibid, rec 20. In August 2006, the OPC launched its layered privacy policy notice. See Office of the Privacy Commissioner, 'Release of Privacy Impact Assessment Guide and Layered Privacy Policy' (Press Release, 29 August 2006) and Office of the Privacy Commissioner, *Privacy Policy* (2006).

78 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Law Council of Australia, *Submission PR 177*, 8 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007.

79 AAMI, *Submission PR 147*, 29 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

> Providing greater detail at the point of collection may, in fact, be counter productive as research shows that many people do not read or do not understand lengthy privacy notices or policies.[80]

24.81 Some stakeholders stated that providing short form privacy notices does not obviate the need also to provide more detailed information, and that 'layered' privacy notices—involving a series of privacy notices that provide differing levels of detail—can be helpful.[81] The OPC submitted that 'more detailed information regarding the personal information management policies of an organisation or agency' should be made available in a separate document to individuals on request.[82]

24.82 On the other hand, while noting that short form privacy notices may be beneficial in certain circumstances, some stakeholders submitted that they should not be mandatory.[83]

24.83 In DP 72, the ALRC proposed that the OPC should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.[84]

24.84 A number of stakeholders supported this proposal.[85] Privacy advocates, however, expressed concerns about the adoption of short form privacy notices. They stated that:

> Many consumer representative organisations, while acknowledging an 'information overload' problem, view trends towards layered and short form privacy notices with suspicion, as they can too easily omit information which should be relevant to an individual's decision whether to proceed with a transaction.

---

80 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007. See also Investment and Financial Services Association, *Submission PR 122*, 15 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007.

81 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; Microsoft Australia, *Submission PR 113*, 15 January 2007.

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

83 See, eg, Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.

84 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007), Proposal 21–5.

85 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; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; Office of the Victorian Privacy Commissioner, *Submission PR 493*, 19 December 2007; Australian Unity Group, *Submission PR 381*, 6 December 2007; Recruitment and Consulting Services Association Australia & New Zealand, *Submission PR 353*, 30 November 2007. Optus noted that it provides short form privacy policies and had 'no objection' to the proposal: Optus, *Submission PR 532*, 21 December 2007.

> We believe that it is necessary to mandate a minimum level of information to be provided at or before the time of collection and a minimum standard of transparency and ease of navigation between specific collection notices and privacy policies. This is best achieved either in Regulations or a binding Code.[86]

24.85 GE Money Australia stated that it is not clear how short form privacy notices work to inform individuals effectively. It said:

> Organisations will be required to have privacy policies, to provide specific notification to individuals and to take certain consents from individuals. Short form privacy notices could be misleading if they do not contain all the information relevant to the organisations proposed handling of personal information in relation to a particular product or service.[87]

ALRC's view

24.86 The OPC should continue to encourage and guide the adoption of short form privacy notices by agencies and organisations. Short form privacy notices serve the useful purpose of communicating, in abridged form, the personal information-handling practices of agencies and organisations. As such, they are more likely to be read and understood by individuals.

24.87 The development of short form privacy notices, however, does not obviate the obligations of agencies and organisations to develop more detailed and comprehensive Privacy Policies. Similarly, agencies and organisations will still be subject to obligations under the 'Notification' principle to ensure that individuals are notified, or otherwise made aware, of specific matters relating to the collection of their personal information.[88] It is possible, however, that the inclusion of a specific matter in a short form notice may be sufficient for the purpose of ensuring an individual is aware of that matter for the purposes of the Notification' principle.

24.88 There is considerable merit in agencies and organisations creating 'layered' privacy notices. This involves making at least two versions of a privacy notice available to individuals—a comprehensive and detailed explanation of the entity's privacy practices, and an abridged version. Both can be made available easily and cheaply in an electronic form, such as via an agency's or organisation's website.

24.89 The creation of short form privacy notices, however, should not be mandated by the privacy principles. First, such an approach is inconsistent with the intention of having high-level principles in the *Privacy Act.*[89] Secondly, it may not be appropriate, practical and necessary for an agency or organisation to develop short form notices in addition to complying with its obligations under the 'Openness' and 'Notification'

---

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

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

88 See Ch 23.

89 See Rec 18–1.

principles. For example, it may be overly burdensome, and render little by way of additional privacy protection, to require a small business that holds a minimal amount of personal information to produce short form notices.

Recommendation 24–3 The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information-handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.

Summary of 'Openness' principle

24.90 The fourth principle in the model UPPs should be called 'Openness'. It may be summarised as follows.

UPP 4. Openness

4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:

(a) sort of personal information the agency or organisation holds;

(b) purposes for which personal information is held;

(c) avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and

(e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

(a) electronically; and

(b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.