The Senate

Finance and Public Administration Legislation Committee

Exposure Drafts of Australian Privacy Amendment Legislation

Part 1 – Australian Privacy Principles

June 2011

ISBN 978-1-74229-473-5

Senate Finance and Public Administration Committee Secretariat:

Ms Christine McDonald (Secretary)

Ms Kyriaki Mechanicos (Senior Research Officer)

Ms Victoria Robinson-Conlon (Research Officer)

Mr Hugh Griffin (Administrative Officer)

The Senate
Parliament House
Canberra ACT 2600

Phone: 02 6277 3439
Fax: 02 6277 5809
E-mail: fpa.sen@aph.gov.au
Internet: http://www.aph.gov.au/senate/committee/fapa_ctte/index.htm

This document was produced by the Senate Finance and Public Administration Committee Secretariat and printed by the Senate Printing Unit, Parliament House, Canberra.

MEMBERSHIP OF THE COMMITTEE

42nd Parliament

Members

Senator Helen Polley, Chair	ALP, Tasmania
Senator Scott Ryan, Deputy Chair	LP, Victoria
Senator Doug Cameron	ALP, New South Wales
Senator Jacinta Collins	ALP, Victoria
Senator Helen Kroger	LP, Victoria
Senator Rachel Siewert	AG, Western Australia

43rd Parliament

Members

Senator Helen Polley, Chair	ALP, Tasmania
Senator Mitch Fifield, Deputy Chair	LP, Victoria
Senator the Hon John Faulkner	ALP, New South Wales
Senator Helen Kroger	LP, Victoria
Senator Rachel Siewert	AG, Western Australia
Senator the Hon Ursula Stephens	ALP, New South Wales

Substitute Member

Senator Scott Ludlam to replace Senator Siewert for the inquiry

Participating Members for this inquiry

Senator the Hon Brett Mason	LP, Queensland
Senator Nick Xenophon	IND, South Australia

TABLE OF CONTENTS

ABBREVIATIONS

AANA	Australian Association of National Advertisers
ABA	Australian Bankers' Association
ADMA	Australian Direct Marketing Association
ADR	alternative dispute resolution
AFC	Australian Finance Conference
AHA	Australian Hotels Association
AICM	Australian Institute of Credit Management
ALRC	Australian Law Reform Commission
AMA	Australian Medical Association
APEC	Asia-Pacific Economic Cooperation
APP	Australian Privacy Principles
CPEA	Cross-border Privacy Enforcement Arrangement
FSC	Financial Services Council
HSC	Health Services Commissioner, Victoria
IPPs	Information Privacy Principles
LCA	Law Council of Australia
LIV	Law Institute of Victoria
NAB	National Australia Bank
NAID	National Association of Information Destruction
NPPs	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
OECD	Organisation of Economic Cooperation and Development
OGCYP	Office of the Guardian for Children and Young People, South Australia
OIC	Office of the Information Commissioner, Queensland
OPC	Office of the Privacy Commissioner
PDS	Product Disclosure Statement
PIAC	Public Interest Advocacy Centre
UPPs	Unified Privacy Principles

RECOMMENDATIONS

Chapter 3 General issues

Recommendation 1

3.30 The committee recommends that the Department of the Prime Minister and Cabinet re-assess the draft Australian Privacy Principles with a view to improving clarity through the use of simpler and more concise terms and to avoid the repetition of requirements that are substantially similar.

Recommendation 2

3.32 The committee recommends that reconsideration be given to the inclusion of agency specific provisions in the Australian Privacy Principles in the light of the Office of the Privacy Commissioner's suggestion that agency specific matters should, in the first instance, be dealt with in portfolio legislation.

Recommendation 3

3.73 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the interpretation of 'personal information' as a matter of priority.

Recommendation 4

3.90 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the meaning of 'consent' in the context of the new Privacy Act as a matter of priority.

Recommendation 5

3.114 The committee recommends that the Government, in consultation with the Office of the Australian Information Commissioner, give consideration to the provision of a transition period for entities to fully comply with the implementation of the new Privacy Act.

Chapter 4 Australian Privacy Principle 1–open and transparent management of personal information

Recommendation 6

4.45 The committee recommends that a note be added at the end of APP 1(5) which indicates that the form of an entity's privacy policy 'as is appropriate' will usually be an online privacy policy.

Chapter 5 Australian Privacy Principle 2–anonymity and pseudonymity

Recommendation 7

5.37 The committee recommends that the wording of APP 2(2)(a) be reconsidered to ensure that the exception to the anonymity and pseudonymity principle cannot be applied inappropriately.

Chapter 6 Australian Privacy Principle 3–collection of solicited personal information

Recommendation 8

6.35 The committee recommends that in relation to the collection of solicited information principle (APP 3), further consideration be given to:

- **whether the addition of the word 'reasonably' in the 'necessary' test weakens the principle; and**
- **excluding organisations from the application of the 'directly related to' test to ensure that privacy protections are not compromised.**

Chapter 7 Australian Privacy Principle 4–receiving unsolicited information

Recommendation 9

7.44 The committee recommends that the term 'no longer personal information' contained in APP 4(4)(b) be clarified.

Chapter 10 Australian Privacy Principle 7–direct marketing

Recommendation 10

10.46 The committee recommends that the drafting of APP 7 be reconsidered with the aim of improving structure and clarity to ensure that the intent of the principle is not undermined.

Recommendation 11

10.60 The committee recommends that the note to APP 7(1) be redrafted to better reflect the position outlined in the Government response.

Recommendation 12

10.66 The committee recommends that the Australian Information Commissioner develop guidance in relation to direct marketing to vulnerable people.

Recommendation 13

10.81 The committee recommends that the structure of APP 7(2) and APP 7(3) in relation to APP 7(3)(a)(i) be reconsidered.

Chapter 11 Australian Privacy Principle 8–cross-border disclosure of personal information and sections 19 and 20

Recommendation 14

11.41 The committee recommends that a note be added to the end of APP 8 making reference to section 20 of the new Privacy Act.

Recommendation 15

11.53 The committee recommends that the Department of the Prime Minister and Cabinet develop explanatory material to clarify the application of the term 'disclosure' in Australian Privacy Principle 8.

Recommendation 16

11.64 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the types of contractual arrangements required to comply with APP 8 and that guidance be available concurrently with the new Privacy Act.

Recommendation 17

11.103 The committee recommends that, when the Australian Government enters into an international agreement relating to information sharing which will constitute an exception under APP 8(2)(d), the agency or the relevant minister table in the Parliament, as soon as practicable following the commencement of that agreement, a statement indicating:

- **the terms under which personal information will be disclosed pursuant to the agreement; and**
- **the effect of the agreement on the privacy rights of individuals.**

Recommendation 18

11.105 The committee recommends that further consideration be given to the wording of the law enforcement exception in APP 8(2)(g) to ensure that the intention of the provision is clear.

Recommendation 19

11.120 The committee recommends that section 19, relating to the extraterritorial application of the Act, be reconsidered to provide clarity as to the policy intent of the provision.

Recommendation 20

11.133 The committee recommends that the Department of the Prime Minister and Cabinet develop explanatory material in relation to the application of the accountability provisions of section 20.

Chapter 12 Australian Privacy Principle 9–adoption, use or disclosure of government related identifiers

Recommendation 21

12.33 The committee recommends that the term 'reasonably necessary' be replaced with 'necessary' in APP 9(2)(a), (b) and (f).

Recommendation 22

12.38 The committee recommends that the Office of the Australian Information Commissioner undertake a review of agency voluntary data-matching guidelines, including emerging issues with the use of government identifiers, and that the outcome inform further consideration of the extension of APP 9 to agencies.

Chapter 13 Australian Privacy Principle 10–quality of personal information

Recommendation 23

13.35 The committee recommends that proposed APP 10(2), pertaining to the quality of personal information disclosed by an entity, be re-drafted to make clear the intended use of the term 'relevant'.

Chapter 14 Australian Privacy Principle 11–security of personal information

Recommendation 24

14.36 The committee recommends that a definition of the term 'interference' used in proposed APP 11(1)(a), pertaining the security of personal information, be provided or a note included in the legislation to explain its meaning in this context.

Recommendation 25

14.38 The committee recommends that the Australian Information Commissioner provide guidance on the meaning of 'destruction' in relation to personal information no longer required and the appropriate methods of destruction of that information.

Chapter 15 Australian Privacy Principle 12–access to personal information

Recommendation 26

15.43 The committee recommends that, in relation to the proposed exceptions provided for in APP 12(3):

- **the Australian Information Commissioner provide guidance in relation to the application of the 'frivolous and vexatious' exception (APP 12(3)(c));**
- **clarity be provided as to the stage at which the negotiations exception in APP 12(3)(e) may be invoked; and**
- **further consideration be given to the exception in APP 12(3)(j) in relation to commercially sensitive decisions to ensure that the rights currently provided for in the *Privacy Act 1988* are not diminished.**

Recommendation 27

15.46 The committee recommends that a note be added to proposed APP 12(4)(a) to clarify that a reasonable period of time in which an organisation must respond to a request for access would not usually be longer than 30 days.

Recommendation 28

15.47 The committee recommends that APP 12(8) be amended so that it is made clear that access charges imposed by organisations should only be charged at a level reasonably necessary to recoup costs incurred by the entity.

Chapter 16 Australian Privacy Principle 13–correction of personal information

Recommendation 29

16.34 That the decision to omit the term 'misleading' in APP 13, relating to the correction of personal information, be reconsidered.

Chapter 1

Introduction

Terms of reference

1.1 On 24 June 2010, the Senate agreed to the following:

> (1) That the following matter be referred to the Finance and Public Administration Legislation Committee for inquiry and report by 1 July 2011:
>
> Exposure drafts of Australian privacy amendment legislation.
>
> (2) That, in undertaking this inquiry the committee may consider the exposure draft of the Australian Privacy Principles and the draft companion guides on the Australian privacy reforms, and any other relevant documents tabled in the Senate or presented to the President by a senator when the Senate is not sitting.

1.2 Following the commencement of the 43rd Parliament, the Senate agreed to the committee's recommendation that the inquiry be re-adopted with a reporting date of 1 July 2011.

Conduct of the inquiry

1.3 On the same day that the inquiry was referred to the committee, the Australian Privacy Principles (APP) Exposure Draft and Companion Guide were tabled in the Senate.[1] The APP Exposure Draft is one of four parts of the first stage response to the Australian Law Reform Commission's (ALRC) recommendations for the reform of Australian privacy laws. The committee agreed that it would report on this first part of the inquiry by 21 September 2010. Following the commencement of the new Parliament, the committee agreed to table the report by the end of the second sitting week in February 2010. This was subsequently extended to allow the committee further time to consider the matters before it.

1.4 The committee advertised the inquiry in *The Australian* and contacted a number of organisations and individuals, inviting submissions to be lodged by 27 July 2010. However, the committee continued to receive submissions during the new Parliament. The committee received 43 public submissions and two confidential submissions. The list of submissions is available at Appendix 1.

1.5 The committee held a public hearing in Canberra on 25 November 2010. Details of the public hearing are at Appendix 2. Following the public hearing, the committee provided the Department of the Prime Minister and Cabinet with an extensive list of questions on notice. The submissions, Hansard transcript of evidence

---

1 *Journals of the Senate*, 24 June 2010, p. 3762.

and answers to questions on notice may be accessed through the committee's website at http://www.aph.gov.au/Senate/committee/fapa_ctte/foi_ic/index.htm.

1.6 The committee would like to thank all those who contributed to the inquiry.

Structure of the report

1.7 The report is structured as follows:

- chapter 2 of the report provides a background to the *Privacy Act 1988*, the inquiry undertaken by the Senate Legal and Constitutional Affairs References Committee into the Privacy Act in 2005, and the reviews by the Office of the Privacy Commissioner and the ALRC;[2]
- chapter 3 canvasses general issues raised in relation to the exposure draft;
- chapters 4 to 16 discuss the key issues raised in relation to each APP together with an overview of the ALRC's comments on each principle; and
- chapter 17 presents a summary of the committee's conclusions.

1.8 The Information Privacy Principles and the National Privacy Principles are provided in Appendix 3 and the exposure draft of the Australian Privacy Principles is provided at Appendix 4.

References

1.9 On 1 November 2010 the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner. The submission from the Office of the Privacy Commissioner (OPC) was received before this change took place and this report therefore refers to the Office of the Privacy Commissioner.

2 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, May 2008, ALRC 108.

Chapter 2

Background

2.1 This chapter provides an overview of the *Privacy Act 1988* (the Privacy Act), the inquiry undertaken by the Senate Legal and Constitutional Affairs References Committee into the Privacy Act and the reviews conducted by the Office of the Privacy Commissioner (OPC) and Australian Law Reform Commission (ALRC).[1]

Privacy Act 1988

2.2 The *Privacy Act 1988* was enacted to give effect to Australia's agreement to implement the Organisation for Economic Cooperation and Development (OECD) *Guidelines for the Protection of Privacy and Transborder Flows of Personal Information*, as well as to its obligations under Article 17 of the International Covenant on Civil and Political Rights.

2.3 The Privacy Act initially regulated the collection, handling and use of information about individuals by Commonwealth Government departments and agencies. The Privacy Act also established the Privacy Commissioner to oversee privacy matters and to handle complaints. In addition, the Privacy Act provided guidelines for the collection, storage, use and security of tax file number information.[2] Eleven Information Privacy Principles (IPPs), based on the OECD guidelines, set out the safeguards for personal information that is handled by the Commonwealth Government and Australian Capital Territory Government agencies.[3]

2.4 Amendments were made to the Privacy Act in 2000 to strengthen privacy protection in the private sector by establishing national standards for the handling of personal information by the private sector. The aim was to give consumers confidence in Australian business practices; to take advantage of the opportunities presented by electronic commerce and the information economy; and allay concerns about the security of personal information when conducting business online. The *Privacy Amendment (Private Sector) Act 2000* provided for approved privacy codes and introduced National Privacy Principles (NPPs). The NPPs were based on voluntary guidelines for the private sector, the National Principles for the Fair Handling of

---

1 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008.

2 The Hon Lionel Bowen MP, Attorney-General, *House of Representatives Hansard*, 1 November 1988, p. 2117.

3 ACT Government agencies became bound by the Privacy Act through the passing of the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994*.

Personal Information, which had been developed by the Privacy Commissioner. The amendments also introduced exemptions for small business and employee records.[4]

2.5 Other amendments to the Privacy Act since 1988 provided the Privacy Commissioner with additional functions in relation to:

- spent convictions;
- regulation of credit reporting and information held by credit reporting agencies and credit providers (1990);
- data matching (1990);
- guidelines to safeguard personal information provided for the purposes of the Pharmaceutical and Medical Benefits Schemes (1991); and
- records made by telecommunications carriers, carriage service providers and others of their disclosures of customer information (1997).

2.6 Further amendments in 2006 were made to the definitions of 'health information' and 'sensitive information' to expressly include genetic information to ensure that the collection, use and disclosure of genetic information would be given the additional protections of the Privacy Act. In addition, new provisions were inserted into the Act to enhance information exchange between Commonwealth Government agencies, State and Territory authorities, private sector organisations, non-government organisations and others, in an emergency or disaster situation.

2.7 On 1 November 2010, the Office of the Privacy Commissioner (OPC) was integrated into the Office of the Australian Information Commissioner (OAIC).

Reviews of the Privacy Act

Senate Legal and Constitutional Affairs References Committee

2.8 In June 2005, the Senate Legal and Constitutional Affairs References Committee tabled its report, *The real Big Brother: Inquiry into the Privacy Act 1988.*[5] The committee's inquiry reviewed the overall effectiveness and appropriateness of the Privacy Act as a means of protecting the privacy of Australians with particular reference to international comparisons and emerging technologies. The committee also reviewed the effectiveness of the extension of the privacy scheme to the private sector and the resourcing of the OPC.

2.9 The committee made 19 recommendations including that the Commonwealth Government undertake a comprehensive review of privacy regulation, including a review of the Privacy Act in its entirety with the objective of establishing a nationally

---

4 The Hon Daryl Williams AM QC, MP, Attorney-General, *House of Representatives Hansard,* 12 April 2000, p. 15749.

5 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005.

consistent privacy protection regime to effectively protect the privacy of Australians. In addition, the Committee recommended that the review be undertaken by the ALRC and that the report be presented to the Government and to the Parliament.

Office of the Privacy Commissioner

2.10 On 13 August 2004, the Attorney-General asked the Privacy Commissioner to review the operation of the private sector provisions of the Privacy Act. In March 2005, the OPC reported on its review.[6] The OPC recommended that the Government consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia.

Australian Law Reform Commission

2.11 On 30 January 2006, the then Attorney-General, the Hon Philip Ruddock, MP, announced that the Australian Law Reform Commission (ALRC) would undertake a comprehensive review of the Privacy Act. The Attorney-General stated the review was being undertaken in response to the recommendations of the Senate Legal and Constitutional Affairs References Committee and the OPC recommendations and commented:

> It is timely to respond to these recommendations and review the overall effectiveness of the Privacy Act to see where improvements can be made…
>
> The Review will examine existing Commonwealth, State and Territory laws and practices and will consider the needs of individuals for privacy protection in light of evolving technology…
>
> The ALRC will also examine current and emerging international law in the privacy area and consider community perceptions of privacy and the extent to which it should be protected by legislation.[7]

2.12 In undertaking the review, the ALRC was to identify and consult with relevant stakeholders, State and Territory Governments, the business community and the public, and report by 31 March 2008. The ALRC was subsequently granted an extension of the reporting date to 30 May 2008.

2.13 The ALRC's report, *For Your Information: Australian Privacy Law and Practice* was the culmination of a 28 month inquiry which included face-to-face meetings with individuals, organisations and agencies; public forums; workshops; and a phone-in.[8] The ALRC also produced two issues papers: *Review of Privacy* (IP 31)

---

6 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005.

7 The Hon Philip Ruddock MP, Attorney-General, *Media Release*, 'Australian Law Reform Commission to Review Privacy Act', 31 January 2006.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008.

and *Review of Privacy: Credit Reporting Provisions* (IP 32); as well as a three-volume Discussion Paper, *Review of Australian Privacy Law* (DP 72).

2.14 The extensive public engagement provided the ALRC with a range of views on privacy issues. For example, there was a general feeling that technological advances had steadily and irreparably eroded personal privacy and that much greater effort should be made to resist this. At the same time, the benefits of information and communication technologies were acknowledged.

2.15 The ALRC also found that there was a high degree of willingness to trade-off privacy interests to meet concerns about law and order at a local level or about national security more generally. In addition, while privacy was frequently seen as a 'right', a need to strike a commonsense balance between privacy interests and practical concerns in a range of areas was acknowledged, one example being the access to sensitive personal health information in the case of a medical emergency.[9]

2.16 Children and young people were consulted during the review and provided an insight into views on privacy in relation to new mediums such as websites like Facebook. The ALRC noted that some young people were very savvy about how to control access to, and distribution of, personal information on social networking sites. Unfortunately, many young people were unaware of how to protect their privacy and the implications of widely distributing, downloading or archiving personal information. The ALRC found that 'there was little appetite for more law or formal regulation in this area'. Rather, the need for more education was emphasised.[10]

2.17 Other issues highlighted in the consultations were the complexity of privacy laws in Australia particularly the overlapping of Commonwealth, State and Territory laws and the separate privacy principles for the public and private sectors; the lack of adequate enforcement mechanisms in privacy legislation; and, the use of 'because of the Privacy Act' as an excuse for inaction or non-cooperation.[11]

2.18 The ALRC made 295 recommendations to improve privacy protection in Australia in the following key areas:

- redrafting and reconstructing the Privacy Act and privacy principles to achieve significantly greater consistency, clarity and simplicity;
- unification of the privacy principles for the public and the private sector into one single set of principles;

---

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 107–08.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 108–09.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 108–09.

- structuring privacy regulation to follow a three-tiered approach: high level principles of general application; regulation and industry codes detailing the handling of personal information in certain specified contexts; and, guidance provided by the Privacy Commissioner dealing with operational matters and providing explanations;
- adoption of a common approach to privacy in all jurisdictions in order to overcome confusion and uncertainty, including the establishment of an intergovernmental cooperative scheme;
- updating of key definitions, including the definitions of 'personal information', 'sensitive information' and 'record';
- improvements to complaint handling;
- rationalisation and clarification of exemptions from, and exceptions to, the requirements of the Privacy Act;
- restructuring of the Office of the Privacy Commissioner and strengthening of the role of the Privacy Commissioner;
- implementation of a data breach notification process;
- clarification of the legal position to facilitate authorised persons to assist a person, temporarily or permanently incapacitated, to deal with agencies or organisations;
- more comprehensive credit reporting requirements;
- promotion of national consistency in relation to health information;
- greater facilitation of research through an exception to the 'Collection' and 'Use and Disclosure' principles in the model Unified Privacy Principles;
- provision of a 'Cross-Border Data Flows' principle to ensure accountability for personal information transferred offshore; and
- provision in federal legislation for a statutory cause of action for a serious breach of privacy.

2.19 The ALRC also recommended that the Commonwealth Government initiate a review of the amended Privacy Act and credit reporting information regulations five years after the date of commencement.

2.20 In addition to the recommendations, the ALRC also provided eleven Unified Privacy Principles (UPPs). The ALRC noted that:

> 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.[12]

Government response to the ALRC review

2.21 In October 2009, the Government provided its first stage response to the ALRC's report. In providing the response, the Cabinet Secretary and Special Minister of State, Senator the Hon Joe Ludwig stated:

> The Government will outline a clear and simple framework for privacy rights and obligations and build on its commitment to trust and integrity in Government. The Government will:
>
> - create a harmonised set of Privacy Principles which will replace the separate sets of public and private sector principles at the federal level, untangling red tape and marking a significant step on the road to national consistency;
> - redraft and update the Privacy Act to make the law clearer and easier to comply with;
> - create a comprehensive credit reporting framework which will improve individual credit assessments, complimenting the Government's reforms to responsible lending practices;
> - improve health sector information flows, and give individuals new rights to control their health records, contributing to better health service delivery;
> - require the public and private sector to ensure the right to privacy will continue to be protected if personal information is sent overseas; and
> - strengthen the Privacy Commissioner's powers to conduct investigations, resolve complaints and promote compliance, contributing to more effective and stronger protection of the right to privacy.
>
> These reforms will be technology neutral, providing protection for personal information held in any medium. The Privacy Commissioner will also have an enhanced role in researching, guiding and educating on technologies that enhance or impact on privacy.[13]

2.22 In formulating the response, the Department of the Prime Minister and Cabinet (the department) conducted further consultations with stakeholders, agencies, industry and consumer representatives, academics and privacy experts. The first stage response addressed 197 of the ALRC's 295 recommendations. The department stated that of those 197 recommendations, the Government:

- accepted 141 recommendations, either in full or in principle;

---

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 638.

13 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, p. 6.

- accepted 34 recommendations with qualification;
- did not accept 20 recommendations; and
- noted two recommendations.[14]

2.23 The Cabinet Secretary indicated that once the first stage reforms had progressed, the remaining recommendations would be considered. It was also noted that the remaining recommendations 'include sensitive and complex questions around the removal of exceptions and data breach notices'. Extensive consultation and input will be required for these matters.

14 Australian Government, *Enhancing National Privacy Protection*, p. 9.

Chapter 3

General Issues

Introduction

3.1 The Australian Privacy Principles Exposure Draft is the first stage of the Government's proposed reform of the privacy regime. The aim of the reform is to implement a streamlined set of unified privacy principles that provide for privacy rights and obligations so as to protect an individual from the risk of harm through inappropriate sharing and handling of their personal information. As stated in the Government's response to the Australian Law Reform Commission's (ALRC) review, 'underpinning the enhanced protection of privacy is a simple and clear framework' that is principles-based.[1]

3.2 This chapter canvasses general issues raised by submitters to the inquiry which principally go to concerns about the complexity and structure of the APPs, the definition of some terms used, and exemptions from the Privacy Act. Other matters discussed include the consultation process undertaken in developing the exposure draft, implications for state and territory governments, the need for a transition period, and the potential compliance and cost burden of the proposed reforms.

Clarity of the Australian Privacy Principles

3.3 The objective of streamlined principles that are clear and easy to understand is fundamental to the privacy regime and was the subject of much comment by submitters. As a first step to this aim, the two existing sets of privacy principles – the Information Privacy Principles and the National Privacy Principles – have been replaced with a single set of unified principles. Professor Rosalind Croucher, President, ALRC, commented on the benefits of such an approach and noted that having one set of principles applying to private sector organisations and one set applying to public sector agencies may cause confusion and that:

> …where there is confusion there is the possibility of an imperfect protection and an imperfect respect for the fundamental protection of personal information. In that context, the development of a unified set of principles would only improve the ability for those governed by it to discharge the responsibility under them.[2]

---

1 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, p. 11.

2 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard,* 25 November 2010, p. 5; see also Office of the Privacy Commissioner, *Submission 39,* p. 13.

3.4 Most submitters supported the unified principles approach. The Australian Institute of Credit Management, for example, commented:

> …this will result in a consistent approach to the management of personal information irrespective of the nature of the entity that is managing the personal information. Further it will facilitate an individual's understanding of how their personal information is to be managed.[3]

3.5 The committee received some positive comments about the drafting of the APPs. The National Association for Information Destruction (NAID-Australasia) for example, commented that the drafters of the APPs have achieved 'a balance between providing clear guidance while not being over prescriptive' and commended the use of 'reasonableness and technological neutrality to achieve this balance'.[4]

3.6 However, other submitters were of the view that the draft APPs are overly complex and lack clarity and do not achieve the aims of high-level principles-based law. Concern was expressed that this may work against accessibility and compliance. The Office of the Privacy Commissioner (OPC) commented that the following factors should be noted in assessing the APPs:

- the importance of clear and accessible language to ensure the overall effectiveness of principle-based privacy law;
- the need for accessibility for individuals to understand and navigate the APPs, often without legal expertise;
- the benefits of simplicity and clarity for agencies and businesses to understand and comply with their obligations (including those small businesses currently covered by the Privacy Act).[5]

3.7 It was also noted that the ALRC had recommended that the privacy principles 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;…
>
> (c) the privacy principles should be simple, clear and easy to understand and apply.[6]

3.8 In its discussion of this objective, the ALRC expressed the view that principles-based regulation should be the primary method used to regulate privacy in Australia. The ALRC noted that a principles-based approach has the advantages of greater flexibility, broader application, a greater degree of 'future-proofing' and has

---

3 Australian Institute of Credit Management, *Submission 8*, p. 1.

4 NAID-Australasia, *Submission 6*, p. 1.

5 Office of the Privacy Commissioner, *Submission 39*, p. 14.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, Recommendation 18–1, p. 653.

considerable stakeholder support.[7] The ALRC did not recommend the adoption of a pure form of principles-based regulation; rather it acknowledged the benefits of allowing principles to be supplemented by more specific rules in regulations or other legislative instruments. In addition, the ALRC stated that 'a primarily principles-based framework can itself adopt varying degrees of detail and prescription within its principles'.[8]

3.9 Professor Croucher, ALRC, also commented:

> So the privacy principles stand as the high-level aspirations and the embodiment of the things that are regarded as the necessary tools to provide or facilitate the protection of personal information at that operational level.[9]

3.10 The Government accepted the ALRC's recommendations for the drafting of the APPs.[10] The Companion Guide commented that the APPs are 'not like other types of legislation' and are principles-based law. It was noted that principles-based law is 'the best regulatory model for information privacy protection in Australia' and that:

> By continuing to use high-level principles, the Privacy Act regulates agencies and organisations in a flexible way. They can tailor personal information handling practices to their diverse needs and business models, and to the equally diverse needs of their clients.
>
> The Privacy Act combines principles-based law with more prescriptive rules where appropriate. This regulation is complemented by guidance and oversight by the regulatory body, the Office of the Australian Information Commissioner.
>
> This is comparable to international regulatory models in Canada, New Zealand and the United Kingdom.[11]

3.11 Submitters argued that the APPs do not achieve the objective of high-level principles nor simplicity. The Office of the Victorian Privacy Commissioner (Privacy Victoria) noted that while some of the APPs are successfully expressed as high-level principles, 'in others the level of detail and complexity work against this aim'. For example, a number of exceptions included in various APPs are specific to Commonwealth agencies. Privacy Victoria concluded that:

> A better approach would be to draft high-level, simple, lucid principles, which could equally apply to Commonwealth, State or Territory public

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 240–41.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 643.

9 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 9.

10 Australian Government, *Enhancing National Privacy Protection*, p. 37.

11 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 9.

> sector agencies, local councils or private sector organisations. Then, where one or more of these entities needed modification to or exemption from the specific APP, this could be done in a separate section of the *Privacy Act*.[12]

3.12 The OPC supported a high-level, principles-based, technology-neutral approach 'that is capable of protecting and promoting individuals' privacy into the future'.[13] The OPC noted that one of the significant benefits of principles-based law is that it is generally easier for the public, and entities with obligations, to understand. Further:

> …principle-based privacy law should enable entities to understand the policy underpinning the law and to adapt their practices accordingly. The law should be clear, but also sufficiently flexible, to enable entities to determine how best to pursue their functions and activities in a way that complies with the Privacy Act.[14]

3.13 The OPC went on to state that clear and easily understood obligations, make it easier for entities to comply, and thereby reduces the administrative burden and cost of compliance and the frequency of privacy breaches and complaints.[15]

3.14 Submitters provided specific examples of APPs which were not considered to meet the aim of high-level principles. The Australian Finance Conference (AFC), for example, commented that APP 8 (cross border disclosure) was substantially different to what was recommended by the ALRC and from the current NPP 9. AFC commented that:

> …as a matter of policy and drafting it fails to achieve the key objectives (e.g. high-level principles, simple, clear and easy to understand and apply) of the reforms. It also shifts the risk balance heavily to the entity and we query the individual interest justification to support that.[16]

3.15 A significant concern raised by submitters was the complexity of some of the APPs. The OPC noted that during its 2005 Private Sector Review stakeholders called for greater simplicity in the drafting of privacy protections. The OPC concluded that the extent to which the exposure draft and APPs achieve the widely supported objectives of high-level principles that are simple and easy to understand 'is an important yardstick for the success of the overall reforms'.[17]

3.16 However, submitters commented that some of the APPs are highly detailed, lengthy, legalistic and complex, with some provisions having to be read in conjunction

---

12 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 2.

13 Office of the Privacy Commissioner, *Submission 39*, p. 5.

14 Office of the Privacy Commissioner, *Submission 39*, p. 15.

15 Office of the Privacy Commissioner, *Submission 39*, p. 15.

16 Australian Finance Conference, *Submission 12*, p. 8.

17 Office of the Privacy Commissioner, *Submission 39*, p. 13.

with other sections to understand how they will apply. It was concluded that the APPs are not clear or easy to understand and apply, contrary to the ALRC's recommendation.[18] The Victorian Privacy Commissioner commented:

> …the current drafting of the APPs works against the simplification and harmonisation which was the core recommendation of the ALRC. The APPs should be redrafted in order to achieve this fundamental objective.[19]

3.17 The Public Interest Advocacy Centre (PIAC) also provided similar comments and argued that a clear and more accessible document should be the aim of the reforms. PIAC stated that this has not been achieved. Rather 'the draft document reads as highly legalistic, and is not designed for easy access by the public'. PIAC noted that the ALRC's recommended principles were approximately 10 pages long, while the APP exposure draft is 41 pages long 'reading often like the most complicated sections of the taxation law'. PIAC concluded:

> Whilst it does appear that the Government has admirably adopted many suggestions made in the consultation process, thereby making the document more complex and qualified, the purpose of having clear privacy principles now appears lost. A plain English redraft is clearly needed.[20]

3.18 Qantas also commented on this matter and submitted:

> Qantas is concerned that the simple language and structure contained in the current National Privacy Principles (NPPs) has been abandoned in favour of a more verbose and complex set of principles which are more difficult to interpret and discern the intention and meaning of.[21]

3.19 The concerns about the effect of complex nature of the APPs were highlighted by the Law Council of Australia (LCA) which commented that it is particularly important for the APPs to be written in plain English, as 'the purpose of the legislation is to give meaning to the privacy rights of individuals'. The LCA was of the view that those outside of the legal profession will be discouraged from engaging with or even reading the APPs. In addition, in their current form, entities are likely to find it difficult to comply with privacy requirements. While it was acknowledged that guidelines would be established by the Privacy Commissioner, the LCA concluded that 'it is also important that the legislation itself is clear and not unwieldy'.[22]

---

18 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 1–2; Law Council of Australia, *Submission 31*, p. 4; Microsoft, *Submission 14*, p. 7; Qantas Airways Limited, *Submission 38*, p. 2; Public Interest Advocacy Centre, *Submission 32*, p. 2; Office of the Privacy Commissioner, *Submission 39*, p. 16.

19 Office of the Victorian Privacy Commissioner (Privacy Victoria), *Submission 5*, p. 12; see also Qantas Airways Limited, *Submission 38*, p. 2.

20 Public Interest Advocacy Centre, *Submission 32*, p. 2.

21 Qantas Airways Limited, *Submission 38*, p. 2.

22 Law Council of Australia, *Submission 31*, p. 4; see also Office of the Privacy Commissioner, *Submission 39*, p. 14.

3.20 In a supplementary submission, the LCA made additional comments in relation to the complexity of the APPs and stated that the APPs should revert to the simpler style of the NPPs which was based on the original OECD guidelines. The LCA added that 'many of the distinctions in the proposed legislation appear unnecessary, making the proposed new principles difficult to interpret, and therefore less accessible to ordinary members of the public at large, to privacy practitioners, regulated organisations and consumers'. The LCA gave examples of the APPs that are more verbose and complex than the NPPs: APP 2 replaces the shorter NPP 8, even though the meaning is essential unchanged.[23]

3.21 The Office of the Guardian for Children and Young People (South Australia) supported the LCA's view and stated that many 'small to medium-sized NGOs would be unable to allocate resources to develop organisational policies and procedures that translate the Principles into operational instruction'.[24]

3.22 Other submitters provided specific examples of where the complexity of the APPs would pose issues with compliance. Privacy Law Consulting, for example, stated that APP 7 (direct marketing) is complex with an equally complex matrix of data types, circumstances and requirements. As a result:

> …organisations will find it difficult to develop compliance programs and systems that can distinguish between, and manage, the matrix of data types, circumstances and requirements. This could result in, for example, organisations simply adopting "the lowest common denominator" (e.g. providing opt-out facilities and/or obtaining consent) in relation to all direct marketing activities, which may be unintended consequences of the principle.[25]

3.23 The OPC provided examples of overly long terms used repeatedly; for example, the use of 'such steps that are reasonable in the circumstances, rather than the shorter, more concise 'reasonable steps'. In addition, the OPC commented that requirements that are substantially similar are repeated, adding to the complexity of the APPs; for example, the requirements relating to the collection of sensitive information in APP 3(2) and (3).[26]

3.24 The many suggestions for simplification of specific APPs are discussed in the relevant chapters of this report. However, the OPC made the following general suggestions to simplify the APPs and make them more readily understandable:

- format the principles in the simpler style used by the ALRC in its Model Unified Privacy Principles (UPPs) or the existing NPPs;

---

23 Law Council of Australia, *Supplementary Submission 31a*, p. 2.

24 Office of the Guardian for Children and Young People, *Submission 4*, p. 6.

25 Privacy Law Consulting, *Submission 24*, p. 4.

26 Office of the Privacy Commissioner, *Submission 39*, pp 16–17.

- use more concise language to reduce length; for example, 'reasonable steps' rather than 'such steps are reasonable in the circumstances';
- avoid repeating requirements that are substantively similar (consider grouping them into one clause);
- consider the plain meaning of terms and use them consistently; and
- keep principles high-level and generally applicable to all entities (rather than to a specific agency or organisation).[27]

3.25 The OPC noted that there were a range of agency specific exceptions throughout the APPs with the first appearing in APP 3. The OPC stated that the APPs 'are intended to provide a broad framework for the appropriate collection, use or disclosure of personal information by agencies and organisations'. Provisions, including the 'required by or authorised by law' provision, take into account the needs of agencies. Rather than agency specific provisions being incorporated in the APPs, the OPC was of the view that it is preferable that the specific activities are addressed in portfolio legislation and commented:

> Keeping the Privacy Act's exceptions generally applicable will maximise the APPs' coherence and relevance to all entities. This is consistent with the recommended objectives that the principles should be 'high-level', and should be redrafted to achieve greater logical consistency, simplicity and clarity.[28]

3.26 The OPC went on to argue that agencies should be aware of existing and new exceptions (for example, the missing persons and the declared emergencies and disasters exceptions) as a means of providing for flexibility for their operations. The OPC also commented that the inclusion of broadly worded exceptions to the general principles could lead to a reduction in accountability of agency activity; for example, the term 'diplomatic or consular functions or activities' could cover a very wide range of activities. The OPC concluded that the inclusion of agency specific exceptions should be limited to instances where there is no appropriate alternative. In addition, it could be considered whether any such exceptions should be accompanied by rules made by the Privacy Commissioner as is envisaged with the missing person exception. The OPC concluded:

> Overall, any such exceptions, or authorisations in other legislation, should balance the agencies' needs to fulfil their functions, with individuals' expectations of personal information protection and agency accountability.[29]

---

27 Office of the Privacy Commissioner, *Submission 39*, pp 6, and 16–17.

28 Office of the Privacy Commissioner, *Submission 39*, p. 28.

29 Office of the Privacy Commissioner, *Submission 39*, p. 30.

Conclusion

3.27 The committee considers that the task faced in drafting a unified set of privacy principles to achieve the Government's aim has been complex and difficult. Drafters were required to consolidate privacy principles covering both agencies and organisations and incorporate the ALRC's recommendations accepted by the Government as well as a broader range of exceptions in some APPs. This has, in some instances, resulted in longer principles. However, the committee does not agree that longer principles are necessarily more complex as has been argued by some submitters.

3.28 The committee supports the view that the APPs must be clear, simple and accessible to all users, not just legal or privacy practitioners. Without an understandable and accessible privacy regime, there is a danger that compliance issues may arise, that effectiveness of the regime may be undermined and that individuals will not adequately understand their privacy rights. The committee has noted the views of the OPC in relation to the need to simplify some aspects of the APPs. As the national privacy regulator, and given its role in investigating complaints, providing advice on privacy rights and providing guidance to agencies and organisations on their new obligations, the committee takes particular note of the OPC's views.

3.29 The committee therefore considers that there are opportunities to refine the APPs to improve clarity and simplicity, particularly in relation to the use of more concise language to reduce the length of the APPs and avoid the repetition of requirements that are substantially similar.

Recommendation 1

3.30 The committee recommends that the Department of the Prime Minister and Cabinet re-assess the draft Australian Privacy Principles with a view to improving clarity through the use of simpler and more concise terms and to avoid the repetition of requirements that are substantially similar.

3.31 A further matter raised in relation to the complexity of the APPs was the inclusion of agency specific provisions. In particular, submitters pointed to the exceptions provided to agencies in some APPs for example, APP 3 (collection of solicited personal information) and APP 8 (cross border disclosure of personal information). The committee acknowledges that the consolidation of the IPPs and NPPs has resulted in the inclusion of agency specific provisions as the privacy regime must include flexibility for particular agencies to carry out their functions. However, the committee notes the comments of submitters that this may affect adversely the objective of establishing high-level principles. The committee therefore believes that reconsideration be given to the inclusion of agency specific provisions in the light of the OPC's suggestion that agency specific matters should, in the first instance, be dealt with in portfolio legislation.

Recommendation 2

3.32 The committee recommends that reconsideration be given to the inclusion of agency specific provisions in the Australian Privacy Principles in the light of the Office of the Privacy Commissioner's suggestion that agency specific matters should, in the first instance, be dealt with in portfolio legislation.

Structure

3.33 The Companion Guide notes that the order in which the APPs appear is intended to reflect the cycle that occurs as entities 'collect, hold, use and disclose personal information.[30] This approach was supported by submitters.[31] The ALRC further commented:

> The manner in which the structure reflects the information cycle also provides great integrity to the structure of the proposed amendments.[32]

3.34 However, Privacy NSW recommended that if the privacy principles are to better reflect the information cycle, and how entities use personal information, APP 10 (quality of personal information) and APP 11 (security of personal information) should be situated after the notification principle (APP 5) and before the use and disclosure principle (APP 6). Privacy NSW commented that the processes of ensuring quality and security of personal information should happen before decisions about use or disclosure of personal information happen.[33]

3.35 Various submitters commented on the inclusion of the APPs within the legislation with each APP forming a separate section of the Act. As a result of this structure, it was noted that the numbering of the sections of the exposure draft is confusing: the number of each APP does not correspond with the section number of the APP. It was recommended that either each APP be numbered the same as the section or clause number, or that the APPs be provided in a schedule to the new Privacy Act.[34]

3.36 Professor Graham Greenleaf and Mr Nigel Waters commented on both these suggestions. They noted that difficulties have arisen in referring to the NPPs as these are located in a schedule to the current Privacy Act. However, they also observed that making each principle a separate section of the Act risks causing confusion. This has

---

30 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 7.

31 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 2; Office of the Privacy Commissioner, *Submission 39*, p. 12; Professor Graham Greenleaf and Mr Nigel Waters, *Submission 25*, p. 5; Microsoft, *Submission 14*, p. 7.

32 Australian Law Reform Commission, *Submission 1*, p. 1.

33 Privacy NSW, *Submission 29*, p. 6.

34 Qantas Airways Limited, *Submission 38*, p. 2; Office of the Privacy Commissioner, *Submission 39*, pp 6 and 22–23; Law Institute of Victoria, *Submission 36*, p. 3; Law Council of Australia, *Submission 31*, p. 4.

occurred with NSW *Privacy and Personal Information Protection Act 1998* where references to the principles and the sections of the NSW Act have been confused. Professor Greenleaf and Mr Waters came to the conclusion that having each principle in a separate section means that 'the Act will work better in online research systems', and that this probably outweighs the difficulties of this approach.[35]

3.37 The Department of the Prime Minister and Cabinet (the department) responded that the numbering 'was a drafting issue' but that it should be remembered that this is the first part of the drafting process and concluded:

> …once the entire Privacy Act is rewritten it will flow and you will see the flow better in terms of the section numbering et cetera.[36]

Conclusions

3.38 The committee considers that the placement of the APPs properly reflect the information cycle. The committee also notes that while the NPPs are listed in a schedule to the Act, the IPPs are included in the Privacy Act. The committee considers that there are advantages in having the APPs within the Act as it places the APPs at the forefront of the legislation and underscores their importance to the reforms envisaged by the Government.

3.39 The committee also notes that section 18 of the exposure draft has been included to ensure that while the APPs are set out in sections, a reference in the Act to an APP by number is a reference to the APP with that number and not the section in which it appears.[37] This makes it clear that the APPs are to be referred to by their number and part rather than by the sections of the Act within which they appear.

3.40 In addition, the committee acknowledges the department's comments that the APP exposure draft is only the first stage of the drafting process.

Technological neutrality

3.41 As indicated in the Companion Guide, the Government agreed with the ALRC's finding that the privacy of individuals will be best protected through a technologically neutral privacy regime.[38]

3.42 The ALRC welcomed the adoption of a technologically neutral approach taken in the exposure draft.[39] Other submitters also agreed that the APPs should be written in such a way as to apply regardless of the specific technology used in the

---

35 Professor Graham Greenleaf and Mr Nigel Waters, *Submission 25*, p. 5.

36 Ms Joan Sheedy, Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 25 November 2010, p. 11.

37 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 8.

38 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 8.

39 Australian Law Reform Commission, *Submission 1*, p. 1.

collection, use and management of personal information.[40] The Australian Direct Marketing Association (ADMA), for example, commented:

> The rapid onset of technologies makes it vitally important that the Australian privacy framework applies and protects personal information regardless of the types of technologies that emerge in the future.[41]

3.43 In the event that a technology is developed in the future that is particularly privacy intrusive, Privacy Victoria argued that specific legislation should be enacted to regulate it effectively.[42]

3.44 The department commented that the ALRC made particular recommendations around keeping the principles and the Act technologically neutral. The department considered that the APPs reflected the Government's agreement with those recommendations, in particular, that the area of technology should be the subject of guidance from the OPC. The department concluded:

> Certainly the government accepted that that was the way to go and not to try to legislate for technology developments because you really cannot. As soon as you do them, you are 10 years out of date immediately.[43]

Conclusions

3.45 The committee considers that the APPs meet the aim of technological neutrality and notes that the Government supports a 'renewed role for the Privacy Commissioner to conduct research, and to guide and educate Australians on technologies that impact on or enhance privacy'.[44]

Definitions and consistency

3.46 The committee received a range of comments in relation to definitions and the consistent use of terms in the APP exposure draft.

Use of the term 'reasonably necessary'

3.47 It was noted that the term 'reasonably necessary' is used extensively in the exposure draft. The OPC submitted that it had a number of 'significant concerns' regarding the use of this term rather than the term 'necessary'. The concerns related to:

---

40 Australian Institute of Credit Management, *Submission 8*, p. 2; Australian Direct Marketing Association, *Submission 27*, p. 2; Microsoft, *Submission 14*, p. 7; The Communications Council, *Submission 23*, p. 5.

41 Australian Direct Marketing Association, *Submission 27,* p. 2.

42 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 2–3.

43 Ms Joan Sheedy, Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 25 November 2010, p. 13.

44 Australian Government, *Enhancing National Privacy Protection*, p. 10.

- the introduction of 'reasonably necessary' in the new collection test in APP 3(1) (APP 3–collection of solicited information);
- multiple interpretations of 'reasonably necessary' in different APPs; and
- varied formulations of tests relating to necessity in the exposure draft.[45]

3.48 The OPC observed that while the Companion Guide states that 'reasonably necessary' is intended to be interpreted objectively, the ALRC report suggested that determining what is 'necessary' is already an objective test. In relation to the use of 'reasonably necessary' in APP 3(1), for example, the OPC considered that it could add a qualification to 'necessary' which unintentionally broadened the scope for collection and thus lessened protections provided in the current IPP and NPP requirements, both of which use 'necessary'. The OPC went on to state that it did not agree that 'reasonably necessary' adds a further objective requirement to APP 3(1) or that such a requirement is needed.[46]

3.49 The second matter noted by the OPC was that there appeared to be different meanings of the term 'reasonably necessary' in different APPs. While the Companion Guide provides an explanation of the term in relation to APP 3(1), the OPC argued that the Companion Guide does not provide guidance about the use of the term in other APPs. For example, the use of 'reasonably necessary' in APP 6(2)(e), which relates to the disclosure of personal information without consent for enforcement related activities, may reflect a different meaning of 'reasonably necessary'. The OPC suggested that 'reasonably necessary' be removed from draft APP 3(1) to minimise confusion and complexity.[47]

3.50 The final matter in relation to the term 'reasonably necessary' raised by the OPC concerned varied formulations of tests involving 'necessary'. The OPC provided a table which shows that APP 3(3) contains three different tests across seven provisions and stated that:

> It may be unclear to an individual, business or agency reading APP 3(3) what the various different formulations mean, which is intended to be more restrictive, and which more permissive.[48]

3.51 While supporting distinctions to add clarity, the OPC argued that the tests could be streamlined so that inconsistent and confusing language is removed.[49] The OPC concluded that, in order to improve clarity and simplicity, the term 'reasonably necessary' be replaced with 'necessary' throughout the APPs and that, if further clarity

45 Office of the Privacy Commissioner, *Submission 39*, p. 17.

46 Office of the Privacy Commissioner, *Submission 39*, pp 18–19.

47 Office of the Privacy Commissioner, *Submission 39*, pp 19–20.

48 Office of the Privacy Commissioner, *Submission 39*, p. 21.

49 Office of the Privacy Commissioner, *Submission 39*, pp 20–22.

is required, an objective test for 'necessary' be included in the Explanatory Memorandum.[50]

3.52 The committee raised this issue with the department which put the view that the while word 'reasonably' qualifies the word 'necessary', it did not do so in an inappropriate way. Rather, the department stated:

> The elements of the test are cumulative. So, first, the proposed activity must, from the perspective of a reasonable person, be legitimate for the entity and the intent of purpose; and then, second, the action has to be genuinely necessary for the entity to pursue the intended function or activity. So you have to think of it in two stages.[51]

3.53 The department went on to state that it saw the 'reasonably necessary' test as enhancing the privacy aspects rather than diminishing privacy protections as argued by some submitters.[52]

Reasonable steps test

3.54 The OPC noted that many of the APPs use the term 'such steps as are reasonable in the circumstances' and that this term is based on the older language of the IPPs while the NPPs use the term 'reasonable steps'. The OPC submitted that it is preferable to use the 'reasonable steps' term for the APPs rather than the term 'take steps as are reasonable in the circumstance' as:

- it is shorter and simpler and would thus reduce complexity and length of most of the APPs;
- it can be implied from a plain reading that 'reasonable steps' has an equivalent meaning to 'such steps as are reasonable in the circumstances' as well being emphasised in explanatory material and the Office's guidance (or if necessary, a note on first use in the APPs);
- organisations are already familiar with the concept of 'reasonable steps', and agencies (currently regulated by the longer terminology) will not need to adjust their practices in moving to 'reasonable steps'; and
- in some APPs, the words '(if any)' are added in cases where it may be reasonable not to take any steps, depending on the circumstances.[53]

---

50 Office of the Privacy Commissioner, *Submission 39*, p. 22.

51 Ms Phillipa Lynch, First Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 25 November 2010, p. 12; see also Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 16.

52 Ms Phillipa Lynch, First Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 25 November 2010, p. 12.

53 Office of the Privacy Commissioner, *Submission 39*, p. 23.

3.55 In response to comments on the use of the term 'such steps as are reasonable in the circumstances', the department stated that in its view, the term used ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question. The department concluded:

> While it is arguable that it is implicit in the expression 'reasonable steps' that the surrounding circumstances must be considered, the changed reasonableness formulation makes this explicit. This Department believes this additional clarity and focus on the circumstances surrounding an entity's specific privacy obligation, will have the overall effect of promoting greater compliance with privacy obligations which will be to the benefit of individuals.[54]

3.56 The Law Council of Australia also commented on the 'reasonable steps' test and noted an inconsistency throughout the APPs, with an entity sometimes required to 'take such steps as are reasonable' and other times required to 'take such steps (if any) as are reasonable'. The Law Council submitted that the latter phrase should be adopted consistently throughout the APPs.[55]

Conclusion

3.57 The committee has noted the comments provided by the Office of the Privacy Commissioner in relation to the use of the term 'such steps as are reasonable in the circumstances'. While the committee agrees that the use of a term to make meaning explicit has benefit, it also adds to the complexity and length of many of the APPs. On balance, the committee leans towards the use of the term 'such steps as are reasonable in the circumstances' to ensure that the meaning is clear. However, the committee suggests that the use of this term should be reviewed in the overall re-assessment of the draft APPs as recommended in recommendation 1.

3.58 In relation to the Law Council's comments on the 'reasonable steps' test, the committee notes that the Companion Guide commented on the requirement to take reasonable steps and stated that:

> In some cases the words "(if any)" are used to ensure that, in that particular case, if there are no steps that an entity needs to take to fulfil its obligations, it need not take any steps.[56]

Definition of 'personal information'

3.59 Following its examination of the meaning of the term 'personal information', the ALRC concluded that, as information handling is highly contextual, a significant margin for interpretation and implementation is created and thus:

---

54 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 5.

55 Law Council of Australia, *Submission 31*, pp 4–5.

56 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 16.

> …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'.[57]

3.60 The ALRC went on to recommend 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'.[58]

3.61 The Government accepted this recommendation and commented that the proposed recommendation did not significantly change the scope of what is considered to be 'personal information'.[59] The Companion Guide provides commentary on the definition of 'personal information' and states that the scope of the definition is not changed; rather there is a conceptual difference revolving around the concepts of 'identity', as used in the current definition, and 'identification', as referred to in the recommended definition.[60] The definition of 'personal information' is as follows:

> ***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[61]

3.62 The LCA commented that the definition of 'personal information' 'is a central definition in that it determines the scope of the whole Act' and that the definition proposed should only be supported if 'it is not intended to change the scope of the existing concept'. Further:

> This should be supported by an express and official statement that would be available to assist in interpretation (under the Acts Interpretation Act) to the effect that the change in drafting was not intended to change the meaning.[62]

---

57 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 309.

58 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 309.

59 Australian Government, *Enhancing National Privacy Protection*, p. 24.

60 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 21.

61 Australian Privacy Principles Exposure Draft, p. 31.

62 Law Council of Australia, *Submission 31*, pp 7–8.

3.63 The ADMA supported the new definition of personal information, in particular the inclusion of a 'reasonable' test, and encouraged inclusion of an explanation of the 'reasonable' test in the Explanatory Memorandum for the new Privacy Act.[63]

3.64 However, some submitters argued that the new definition of 'personal information', and the explanation provided in the Companion Guide, have the potential to substantially expand the scope of what is classified as 'personal information', and thereby the scope of what is covered by the Act.[64] Submitters argued that an expanded scope of personal information would result in more onerous requirements on entities, and potentially an increased cost burden.[65]

3.65 Submitters were concerned to ensure that any expansion of scope is clearly expressed either in the legislation or in the explanatory material accompanying the legislation. Google, for example, commented:

> ...the legislation should itself make clear that the context and circumstances in which information is held is to be taken into account in determining whether information is or is likely to be aggregated or combined so as to enable an individual to be reasonably identifiable.[66]

3.66 Yahoo!7 and the Law Institute of Victoria (LIV) commented on the inclusion of 'opinion' in the definition of personal information. Yahoo!7 considered that the concept of 'information' is broad enough to incorporate 'opinion' and therefore did not believe that it was necessary to include 'opinion' in the definition.[67]

3.67 The LIV expressed the view that while the APPs currently define 'personal information' as both information and opinions about a person, this should be split into two categories in order to specifically address the issue of ownership and control of personal information. The two categories would be:

- 'primary personal information' which might include identity information, biometric information etc, and which would be owned by the individual, so that the individual can require an entity to destroy primary personal information which it holds about them (subject, of course, to any statutory obligations or rights of entities to collect or retain information); and

---

63 Australian Direct Marketing Association, *Submission 27*, p. 8; see also Microsoft, *Submission 14*, pp 7–8.

64 Australian Association of National Advertisers, *Submission 21*, p. 6; Microsoft, *Submission 14*, pp 7–8; Communications Council, *Submission 23*, p. 6.

65 Microsoft, *Submission 14*, p. 8; Australian Hotels Association, *Submission 22*, p. 3; The Communications Council, *Submission 23*, p. 6.

66 Google Australia Pty Limited, *Submission 16*, p. 8; Law Institute of Victoria, *Submission 36*, p. 3.

67 Yahoo!7, *Submission 20*, p. 3.

- 'secondary personal information', which would be opinions held about an individual.[68]

3.68 Submitters also provided suggested amendments to the definition of 'personal information' as follows:

- Privacy NSW recommended that the words 'from the information or opinion' be added after 'reasonably identifiable' to provide the appropriate context;[69]
- Privacy NSW recommended that the definition exclude certain categories of information, such as information more than 30 years old, as is the case in the NSW privacy legislation, thus removing repeated references to the exclusions;[70]
- Professor Graham Greenleaf and Mr Nigel Waters submitted that the definition needs to be broadened by replacing 'reasonably identifiable' with 'potentially identifiable' to ensure that the Act covers 'information which, while not in itself identifying an individual, allows interaction with persons on an individualised basis, or the imparting of consequences on an individualised basis';[71] and
- Yahoo!7 also argued that as a person could be reasonably identifiable to one entity and not another, the phrase 'by an entity' be added to the first sentence of the definition so that it encompassed an individual who is 'reasonably identifiable by an entity'. For example, 'an IP address could be considered personal information by an ISP as they are capable of reasonably identifying the person to whom that IP address resolves back to. An online services provider who does not offer Internet access will not be able to use an IP address to identify a person'.[72]

3.69 Submitters supported the recommendation that the OPC develop guidance on the interpretation of 'personal information' to assist entities in ensuring that they have appropriate processes in place for their functions and activities to comply with the Act.[73]

3.70 The department provided a detailed response to concerns raised in relation to the term 'personal information'. The department noted that inclusion of the requirement that the individual be 'reasonably identifiable' ensures that the definition

---

68 Law Institute of Victoria, *Submission 36*, p. 3.

69 Privacy NSW, *Submission 29*, p. 2.

70 Privacy NSW, *Submission 29*, p. 3.

71 Professor Graham Greenleaf and Mr Nigel Waters, *Submission 25*, p. 3.

72 Yahoo!7, *Submission 20*, p. 3.

73 Australian Association of National Advertisers, *Submission 21*, p. 6; Yahoo!7, *Submission 20*, p. 5; Google Australia Pty Limited, *Submission 16*, p. 8; Microsoft, *Submission 14*, pp 7–8; Communications Council, *Submission 23*, p. 6.

continues to be based on factors which are relevant to the context and circumstances in which the information is collected and held. Generally, this would mean that the information must be able to be linked to other information that can identify the individual thus limiting possible identification based on the context and circumstances. In effect, while it may be technically possible for an entity to identify a person by the information it holds, it may be that it is not practically possible. The department concluded that the 'test requires consideration of all the means that are reasonably open for an information holder to identify an individual'.[74]

3.71 The department reiterated that the inclusion of a 'reasonably identifiable' element within the definition does mean that additional information could fall within the new definition. It went on to state:

> Some information on its own would not meet the current definition which requires an individual's identity to be apparent or reasonably ascertainable, from the information (e.g. an IP address). However, that information would fall within the new definition if, in conjunction with other information, it could be used to identify an individual. On that basis, it is arguable that additional information would be subject to the privacy protections in the APPs.
>
> Nevertheless, as noted in the Companion Guide, the proposed definition of 'personal information' does not significantly change the scope of the existing concept in the existing Privacy Act. The key conceptual difference revolves around the concepts of 'identity' as used in the current definition, and 'identification' as referred to in the draft definition. The ALRC considered that 'identification' was more consistent with international language and international jurisprudence, and that explanatory material based on the terms 'identified' and 'identifiable' will be more directly relevant.[75]

Conclusion

3.72 The committee has noted the divergence of views in relation to the definition of 'personal information' and agrees that guidance on this matter should be provided as a matter of priority.

Recommendation 3

3.73 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the interpretation of 'personal information' as a matter of priority.

74 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 2.

75 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, pp 2–3.

The term 'Australian law'

3.74 Both Qantas and Google commented on the definition of, and use of, the term 'Australian law'. This term is used in a number of APPs including APPs 2, 3, 5, 6, 8, 9, 11 and 12. The Companion Guide states that the definition of 'Australian law' is new and 'has been included to clarify the scope of provisions that allow collection, use or disclosure where it is required or authorised by or under law'.[76]

3.75 Qantas commented that confining laws to 'Australian law' fails to recognise that organisations operating in foreign jurisdictions are often required to collect, disclose and use personal information under the laws of those jurisdictions.[77] Google raised the same matter and provided the example of where a foreign country may mandate disclosure of personal information in response to a subpoena issued by a court exercising jurisdiction over the operations of the service provider in that foreign country. In papers submitted by Macquarie Telecom, the storage of data offshore by Australian businesses was examined and it was concluded that 'it is possible that storing data within the United States may provide enough of a connection for a United States court to find jurisdiction over an Australian company storing its data there and subject the company to the US discovery obligations'. Further, data stored in the United States is at greater risk of being accessed by government agencies as the Patriot Act provides US government agencies with extensive powers.[78]

3.76 Google commented that it would be inappropriate to place the service provider in jeopardy under Australian law for responding to a valid court process in a foreign jurisdiction.[79]

3.77 Both Qantas and Google recommended amendment of the exposure draft so as to recognise that entities may need to deal with personal information in ways required under laws of other jurisdictions and that such dealings should not be regarded as an interference with the privacy of an individual under Australian law. Qantas submitted that the appropriate means of achieving this was to replace the term 'Australian law' with the term 'applicable law', being laws (including legislation, regulations, directions and rules) applicable in a relevant jurisdiction.[80]

3.78 The department responded to these concerns as follows:

> The Government's position is that an entity with an Australian link must comply with the APPs relating to an act done, or practice engaged in, within Australia. The existing policy achieved by subsection 6A(4) and section 13D of the Privacy Act will be retained to ensure that an act or

76 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 20.

77 Qantas Airways Limited, *Submission 38*, p. 4.

78 Macquarie Telecom, *Submission 43*, Attachment 1, pp 5–7.

79 Google, *Submission 16*, p. 7.

80 Qantas Airways Limited, *Submission 38*, p. 4.

> practice that is done or engaged in outside Australia will not be an interference with privacy if it is required by an applicable law of a foreign country. For example, an organisation would not breach the APPs if a foreign court judgment required disclosure of personal information in that jurisdiction to assist in investigating a criminal offence.[81]

Conclusion

3.79 The committee notes the advice provided by the department and has no further comment to add in relation to the use of the term 'Australian law'.

Consent

3.80 The ALRC considered 'consent' as it applies to the privacy principles in the Privacy Act and other issues concerning 'consent'.[82] In considering how best to clarify the meaning of 'consent' in relation to privacy, the ALRC did not support the option to amend the Privacy Act to set out in detail what is required to obtain consent as this approach would require a very large number of prescriptive rules. This would also be inconsistent with a principles-based approach. Similarly, amending the definition of 'consent' was not supported as the ALRC noted that the common law has an important role to play in determining elements of consent and a statutory definition would not capture the evolution of the meaning of 'consent' and may have unintended consequences.[83]

3.81 The ALRC formed the view that 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. According to the ALRC, such guidance should address the factors to be taken into account by entities in assessing whether 'consent' has been given. The guidance should also cover express and implied consent as it applies in various contexts; for example, in transactions concerning financial services as well as 'bundled consent'.[84]

3.82 Professor Croucher, President, ALRC, further commented:

> In our report we recommended that the Office of the Privacy Commissioner should develop and publish guidance about what is required of agencies and organisations to obtain an individual's consent. This guidance should, for instance, address a number of the things that I am grabbing at—the factors to be taken into account by agencies and organisations in assessing whether

81 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 2.

82 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 667–88.

83 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 684.

84 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 686.

> it has been obtained, which is kind of what you are asking about in asking how. It should cover express and implied 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—in other words, a consent to general use.[85]

3.83 The Government response indicated that it encouraged the Privacy Commissioner to develop guidance as recommended by the ALRC. In addition, the response indicated that the definition of 'consent' would be expanded to clarify that an individual may withdraw consent where it is lawful to do so.[86] The Companion Guide notes that term 'consent' is defined within the existing Privacy Act and the new Privacy Act will contain a definition on the same terms, that is, that 'consent' means express or implied consent. The Companion Guide goes on to note that there are some circumstances where it will not be possible for a person to withdraw their consent.[87]

3.84 The issue of the definition of 'consent' was raised by some submitters. Both Privacy NSW and the LIV suggested that the definition of 'consent' be further developed. The LIV commented that individuals cannot consent to the collection of sensitive personal information where consent is obtained in a coercive or unreasonable way. The current definition does not preclude consent being obtained unreasonably or in a way that undermines the objectives or purpose of the APPs and should therefore be further developed.[88]

3.85 Privacy NSW argued that separate definitions of, and references to, both 'implied consent' and 'express consent' are required as, under the existing definition, entities may inappropriately rely on implied consent rather than express consent.[89] In particular, Privacy NSW considered that the collection of sensitive information should be contingent on 'express consent' unless the entity can reasonably rely on a relevant exception. Further:

> In circumstances where an individual lacks the capacity to provide express consent (for instance through disability or age), we suggest that there be an exception which permits collection if the entity has obtained express consent from an authorised representative who is empowered to make substitute decisions on behalf of the individual. We suggest that there be an Australian Privacy Rule which governs the means by which an entity be satisfied it is dealing with an authorised representative.[90]

---

85 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 7.

86 Australian Government, *Enhancing National Privacy Protection*, p. 38.

87 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 17.

88 Law Institute of Victoria, *Submission 36*, p. 5.

89 Privacy NSW, *Submission 29*, p. 2.

90 Privacy NSW, *Submission 29*, p. 2.

3.86 The Public Interest Advocacy Centre called for the use of the phrase 'express and informed consent' throughout the APPs.[91]

3.87 Professor Greenleaf and Mr Waters viewed the meaning of 'consent' as critical to privacy policy, but argued that the Government, and indeed the ALRC, had not addressed 'one of the most significant weaknesses in the current regime'. The main concern was that the interpretation of 'consent' could be undertaken in ways that weaken the legislation by undermining the effect of a number of principles. They argued that the concept of 'consent' is crucial and should not be left to guidance by the Privacy Commissioner. Rather, the definition should be amended to deal with key issues and other aspects should be included in the Explanatory Memorandum. Professor Greenleaf and Mr Waters considered that the following points should be made clear:

- consent must be clear and unambiguous, regardless of whether it is express or implied;
- a failure to opt out, on its own, should not be taken as unambiguous consent;
- where an individual must disclose personal information to receive a benefit, no consent can be implied for use beyond the purpose of collection – only express consent should apply; and
- every proposed purpose of use should require separate consent, to prevent the misuse of the practice of 'bundled consent'.[92]

3.88 In its response to the committee's questions on notice in relation to consent, the department commented that under section 15 of the exposure draft, 'consent' means 'express consent or implied consent' and that the Privacy Commissioner has previously stated that implied consent 'arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation'. The department also stated:

> The Government accepted the key thrust of [the ALRC's consent] recommendation and stated that it would encourage the development and publication of appropriate guidance by the Office of the Australian Information Commissioner (AIC), noting that the decision to provide guidance is a matter for the AIC.
>
> While it is ultimately a matter for the AIC, we anticipate that the guidelines will address matters such as those raised by the Law Council of Victoria.[93]

91 Public Interest Advocacy Centre, *Submission 32*, p. 1.

92 Professor Graham Greenleaf and Mr Nigel Waters, *Submission 25*, p. 3.

93 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, February 2011, p. 1.

Conclusion

3.89 The issue of a definition of 'consent' was raised by many submitters. The committee notes the Government's acceptance of the ALRC's recommendation in relation to consent and considers that the matter of consent should be considered by the Office of the Australian Information Commissioner as a matter of priority to ensure that appropriate guidance is available concurrently with the new Act.

Recommendation 4

3.90 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the meaning of 'consent' in the context of the new Privacy Act as a matter of priority.

Exemptions

3.91 A number of submitters commented on the way in which the exposure draft dealt with the issue of exemptions, in particular the continuation of the small business exemption. In the APP exposure draft, the definition of organisation explicitly excludes 'a small business operator' and 'a registered political party', but the exposure draft does not include an express reference to the exemption regarding employee records.[94] Further, the Companion Guide states that the small business exemption will be retained for the time being; however, the Government will consider whether the exemption should continue in its second stage response to the ALRC's review.[95]

3.92 In its submission to the committee, the ALRC reaffirmed its view that the exemptions under the current Privacy Act, pertaining to small business, registered political parties, and employee records, should be removed.[96]

Small business exemption

3.93 A number of submitters called for the removal of the small business exemption.[97] The ALRC commented that:

> …beginning from first principles there is no logical reason why somebody whose personal information is held by a small business should have less privacy protection than somebody who works for a larger enterprise. I would rather put the emphasis on privacy. As a right, obviously, all rights

94 *Australian Privacy Principles Exposure Draft*, s. 17; and Australian Law Reform Commission, *Submission 1*, p. 5.

95 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 6.

96 Australian Law Reform Commission, *Submission 1*, pp 3–6.

97 Australian Law Reform Commission, *Submission 1*, pp 3–4; Dr Colin J Bennett, *Submission 11*, p. 1; Office of the Information Commissioner, Queensland, *Submission 18*, p. 8; Australian Association of National Advertisers, *Submission 21*, pp 7–8; Privacy NSW, *Submission 29*, p. 6; Law Institute of Victoria, *Submission 36*, p. 9.

> have to be balanced, including against economic and financial considerations, but that was always where our emphasis lies.[98]

3.94 Submitters also pointed out that small business is the majority business type in Australia, and, with the use of computer systems, small businesses are able to collect, use and disclose relatively vast amounts of personal information some of which may be very sensitive personal information.[99] Further, it was observed that government entities often outsource services involving personal information, and protection is required when personal information is passed on to the private and community sectors.[100]

3.95 The LIV summed up the position of those who did not support the retention of the exemption by stating that 'the nature of information collected, and not the size of the organisation that collects the information, should determine whether restrictions should be imposed on the collection of information.' The LIV further argued that the exemption does not currently diminish the regulatory burden on small business.[101]

3.96 The ALRC noted that the cost of compliance with the legislation was a significant concern for the small business community, who staunchly supported the retention of the exemption. However, the ALRC observed that small businesses are not exempt from the general privacy law in any 'other comparable jurisdiction in the world'. Further, other stakeholders to the ALRC's review argued that 'consumers have the right to expect that their personal information will be treated in accordance with the privacy principles'. Given this support, the ALRC maintained its recommendation that the small business exemption be removed.[102] The ALRC also noted that its research had shown that the compliance costs may not be as great as previously suggested and that the costs of continuing the exemption in relation to international business may outweigh the compliance costs. Professor Croucher, ALRC, stated:

> The costs as presented to us at the time and as analysed by our own independent research study were not as great as were suggested, and the international context and the standing of our business community within the context of the European directive was such that retaining the exemption, we thought, was not justified.[103]

---

98 Mr Bruce Alston, Senior Legal Officer, ALRC, *Committee Hansard*, 25 November 2010, p. 2.

99 Dr Colin J Bennett, *Submission 11*, p. 1; Australian Association of National Advertisers, *Submission 21*, pp 7–8; Office of the Information Commissioner, Queensland, *Submission 18*, p. 8.

100 Office of the Information Commissioner, Queensland, *Submission 18*, p. 8.

101 The Law Institute of Victoria, *Submission 36*, p. 9.

102 Australian Law Reform Commission, *Submission 1*, pp 3–4.

103 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 3.

3.97 Other submitters supported the retention of the exemption, arguing that removal of the small business exemption would impose an additional compliance and cost burden to small business, which is already subject to significant regulation. It was also noted that there is provision for small businesses to opt-in to the application of privacy legislations, and many small businesses do so. Further, the Australian Hotels Association (AHA) supported the indexation of the current $3 million annual turnover threshold, as fewer small businesses qualify for the exemption every year.[104]

3.98 The Catholic Education Office of the Archdiocese of Melbourne noted that the small business exemption is currently inconsistently applied between Catholic schools. They submitted that an exemption excluding application of the Privacy Act to Catholic schools should be provided, as:

> A Catholic school is not technically a 'business' in the normal commercial sense. It does not strive to make a profit. It is supported by the considerable voluntary efforts of the school community and the Catholic Church and relies heavily on government funding for its revenue. The annual turnover amount is an arbitrary sum, and in many cases the actual turnover of the school varies from year to year, often around the exemption limit.[105]

Registered political parties

3.99 The ALRC also recommended the removal of the exemption for registered political parties both in report and its submission to the committee. While a similar exemption exists in the United States and Canada, registered political parties are not exempt in the United Kingdom, New Zealand or Hong Kong.[106] Professor Croucher, ALRC, commented:

> The fundamental principle is the importance of the protection of personal information. Consistent with the very first principle identified in the Australian Privacy Principles, the 'open and transparent management of personal information', there should not be an exemption of the kind that is contemplated by the political party exemption.[107]

Employee records

3.100 Under the current Privacy Act, employee records are treated differently by agencies and by organisations. While the existing Act does not require Government agencies to treat employees' records any differently to other personal information, private sector organisations are exempt from the requirements of the Privacy Act where their acts or practices relate directly to an employee record held by the

---

104 Australian Hotels Association, *Submission 22*, p. 2; Communications Council, *Submission 23*, p. 9.

105 Catholic Education Office, Archdiocese of Melbourne, *Submission 35*, p. 1.

106 Australian Law Reform Commission, *Submission 1*, pp 4–5.

107 Professor Rosalind Croucher, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 4.

organisation, or the employment relationship between an individual and the organisation. The basis of the exemption of employee records in the private sector is that the protection of such information is more properly a matter for workplace relations legislation.[108]

3.101 In its submission to the committee, the ALRC again called for the removal of the employee records exemption. The ALRC noted that 'there is no sound policy reason why privacy protection for employee records is available to public sector employees but not private sector employees'. Further, as the majority of Australian employees were employed in the private sector, the ALRC considered the exemption resulted in 'a significant gap in privacy regulation'.[109] This position was supported by Privacy NSW.[110]

3.102 The AHA argued for the retention of the exemption, as the collection of information about employees for purposes directly related to their employment is both reasonable and necessary:

> Practices such as surveillance measures to prevent theft or even 'mystery shopper' activities designed to improve service standards are common practices in the industry which require the collection of personal information for the purposes of managing the employment relationship. Records of discussions held with employees over performances matters typically include personal information as defined in the Draft Principles. The maintenance of these sorts of records are necessary under workplace relations legislation if the employer needs to discipline or terminate the employee. It should be mentioned that these same records are also used to determine whether an employee is fit for promotion or an increase in remuneration.[111]

Conclusion

3.103 The committee notes that Companion Guide indicates that, at this stage, the small business exemption will be retained. Ms Joan Sheedy, Department of the Prime Minister and Cabinet, stated that in the second stage response to the ALRC recommendations, the Government will consider the recommendations relating to the removal of the exemptions currently in the Act. Ms Sheedy went on to comment that 'there are no government decisions that have been taken yet in relation to those exemptions'.[112]

---

108 Australian Law Reform Commission, *Submission 1*, p. 5.

109 Australian Law Reform Commission, *Submission 1*, pp 5–6; see also Professor Rosalind Croucher, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 5.

110 Privacy NSW, *Submission 29*, p. 6.

111 Australian Hotels Association, *Submission 22*, p. 2.

112 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 6; Ms Joan Sheedy, Department of the Prime Minister and Cabinet, *Committee Hansard*, 25 November 2010, p. 12.

3.104 The committee considers that no further comment is required at this stage in relation to exemptions from the Privacy Act.

Interaction with state and territory legislation

3.105 Both the Office of the Victorian Privacy Commissioner and the Health Services Commissioner, Victoria (HSC), noted that the Companion Guide indicates that no changes will be made to the Privacy Act provisions which preserve the effect of any state or territory law that makes provisions about interferences with privacy, if it is capable of operating concurrently with the existing Privacy Act. However, they argued that this statement suggests that the approach outlined in the Companion Guide does not reflect the ALRC review recommendations or the approach outlined in the Government response, particularly in relation to private sector health providers.[113]

3.106 While the HSC welcomed the Government's position, as it argued that the interests of consumers and organisations can best be served by having State and Commonwealth regulators working co-operatively, the Office of the Victorian Privacy Commission sought clarity on this issue.[114] Other submitters expressed disappointment that the reforms had not led to a streamlining and harmonisation of privacy law in Australia.[115] Yahoo!7, for example, commented that a level of uncertainty had been introduced 'as we were hoping to operate under a single unified privacy regulation framework'.[116] ADMA went further and stated that the harmonisation:

> …should not be done half heartedly and that states and territories should not be permitted to create other, isolated privacy requirements. The benefit to Australian business of knowing, without doubt, that all privacy requirements are stated in a Commonwealth Privacy Act will to a large extent be undone if this is permitted to occur.[117]

Conclusion

3.107 The committee notes that it is stated in the Government response that 'there are clear benefits of nationally consistent privacy regulation in the private sector, including the health sector'.[118] The department also indicated that the first stage response will create a platform from which the Commonwealth Government can

---

113 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 11; Health Services Commissioner, Victoria, *Submission 26*, p. 6.

114 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 11; Health Services Commissioner, Victoria, *Submission 26*, p. 6.

115 Law Council of Australia, *Submission 31*, p. 4.

116 Yahoo!7, *Submission 20*, pp 4–5.

117 Australian Direct Marketing Association, *Submission 27*, p. 10.

118 Australian Government, *Enhancing National Privacy Protection*, p. 21.

pursue national harmonisation through discussion with state and territory governments. Further:

> All parties to those discussions will need to carefully consider what changes are necessary to their respective privacy and information-sharing regimes to ensure an effective harmonised system can be implemented.[119]

3.108 The committee considers that the harmonisation of privacy regimes across all jurisdictions is an important goal. However, the matters to be considered are complex with examination of interactions with, and possible inconsistencies between, Commonwealth and state and territory regimes requiring detailed examination.

Implementation

3.109 A number of submitters were concerned to ensure that the implementation process for the new Privacy Act includes an appropriate transition period. It was argued that an adequate transition period would allow for the implementation of any necessary systems changes, staff training and updating of relevant corporate policies required to comply with new obligations.[120] The Insurance Council of Australia, for example, commented that the most common method of notifying insurance policyholders of information is through the Product Disclosure Statement (PDS) that is required under the *Corporations Act 2001*. The Council suggested an 18 month transition period would allow general insurers to incorporate any required additional notifications in their PDSs in the normal course of them being re-issued.[121] Other submitters called for a transition period of 12 or 18 months duration.

3.110 The AHA noted that following the amendments to the Privacy Act in 2001, the private sector was granted a 12 month 'amnesty', and submitted that a similar transition period should be granted to the business community/entities following the passage of these amendments.[122]

3.111 Some submitters also specifically stated that requirements under the new legislation should only be applied prospectively.[123]

3.112 The AHA also suggested that an education and awareness campaign will be required to assist acceptance and compliance with the new obligations. Such a

---

119 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, pp 4–5.

120 Financial Services Council, *Submission 34*, p. 4; Australian Hotels Association, *Submission 22*, p. 4; Australian Association of National Advertisers, *Submission 21*, p. 4; Westpac Group, *Submission 13*, pp 1–2.

121 Insurance Council of Australia, *Submission 17*, p. 2.

122 Australian Hotels Association, *Submission 22*, p. 4; The Westpac Group, *Submission 13*, pp 1–2; Insurance Council of Australia, *Submission 17*, pp 1–2.

123 Financial Services Council, *Submission 34*, p. 4; The Westpac Group, *Submission 13*, p. 2.

campaign could be conducted by the Commonwealth in conjunction with relevant industry associations.[124]

Conclusion

3.113 The introduction of the reformed privacy regime may require significant change to practices and policies. The committee considers that due consideration should be given to the provision of an adequate transition period where appropriate. The committee further considers that the Office of the Australian Information Commissioner should be consulted in relation to the length of time of any transition period.

Recommendation 5

3.114 The committee recommends that the Government, in consultation with the Office of the Australian Information Commissioner, give consideration to the provision of a transition period for entities to fully comply with the implementation of the new Privacy Act.

Consultation

3.115 The ALRC undertook extensive consultation during its review of privacy law as did the Government in formulating its response to the ALRC's recommendations. However, the committee received comments in relation to consultations during the development of the exposure draft. The Australian Privacy Foundation (APF) for example, expressed concern that the exposure draft details had 'not been negotiated with a body that includes representatives of all interested parties'. The APF was of the view that the exposure draft reflects the interests of the private sector and government agencies.[125]

3.116 The committee notes, however, that Privacy NSW and the Public Interest Advocacy Centre indicated that they had provided submissions in response to the Government's consultation on the Unified Privacy Principles and related matters.[126] The OPC further noted that it had provided 'informal input' during the development of the exposure draft of the APPs and acknowledged the constructive engagement of the department and its effort to take account of suggestions.[127]

3.117 The committee is satisfied that the department undertook adequate consultation in relation to the APP exposure draft.

---

124 Australian Hotels Association, *Submission 22*, p. 4.

125 Australian Privacy Foundation, *Submission 33*, p. 1.

126 Privacy NSW, *Submission 29*, p. 1; Public interest Advocacy Centre, *Submission 32*, p. 1.

127 Office of the Privacy Commissioner, *Submission 39*, p. 12.

Chapter 4

Australian Privacy Principle 1–open and transparent management of personal information

Introduction

4.1 Australian Privacy Principle 1 (APP 1) addresses open and transparent management of personal information. The Companion Guide states that the requirement for open and transparent management is the first APP because 'it will emphasise that entities should first plan ***how*** they will handle personal information before they collect and process it'. In addition, it will make sure that entities consider their privacy obligations when planning new systems. The Companion Guide noted that this reflects international moves towards a 'privacy by design' approach, so that information systems include privacy and data protection compliance from their inception.[1]

Background

4.2 In its review, the Australian Law Reform Commission (ALRC) considered the openness requirements of the privacy regime. The ALRC concluded that there should be a discrete principle requiring an agency or organisation to operate openly and transparently by providing general information on how it manages personal information. It was noted that compliance with openness requirements generally benefits the regulatory system as a whole and 'therefore, plays a key role in promoting best practice in the handling of personal information'.[2] In addition, the development and publication of privacy policies will promote accountability and increase the transparency of the information handling practices of entities.

4.3 Although both the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) set out openness requirements, openness is achieved by different regulatory mechanisms for agencies and organisations. The ALRC was of the view that there should be one consolidated and simplified openness requirement and stated:

> 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.[3]

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, p. 9.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 810.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 812.

4.4 The ALRC also considered the content of a privacy policy. While the NPPs impose a general obligation to maintain a privacy policy document, the IPPs take a more prescriptive approach and list specific matters to be included in the record summarising how an agency handles personal information.[4] The ALRC concluded that the essential content of a privacy policy should be expressed in high-level terms. The ALRC was of the view that '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'. In addition, any matters required in a privacy policy should not be regarded as being exhaustive.[5]

4.5 The ALRC considered specific matters to be included in a privacy policy and recommended that the list of matters should be limited, but include the sort of personal information held, and the purpose for which that information is held. Other matters required in a privacy policy included the steps available to an individual to access and correct personal information and avenues for complaint.[6]

4.6 The mechanisms for making privacy policies available were canvassed in the review, with the ALRC commenting that loading policies onto websites was 'an ideal mechanism for making them generally available'. In addition, the ALRC recommended that hard copies should be made available on request or in a form accessible for those with special needs.[7]

4.7 The development of short form privacy notices was also examined. The ALRC concluded that short form privacy notices serve a useful purpose and recommended that the Office of the Privacy Commissioner (OPC) should continue to encourage and assist entities to make these available.[8]

Government response

4.8 The Government accepted the ALRC's recommendations in relation to the availability of privacy policies and the development of short form privacy notices and accepted, with amendments, the ALRC's main recommendation in relation to a single openness principle and the matters to be included in a privacy policy.

---

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 813.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 819.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 821–22.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 822–25.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 825–29.

4.9 The Government response stated:

> The Government agrees that organisations and agencies should consider their personal information handling policies and practices and clearly set these out in a Privacy Policy available to all individuals. This helps to promote transparency in the handling of personal information, as well as consumer control, choice and trust in how their information will be handled.
>
> The Government also agrees that requiring agencies and organisations to express in their Privacy Policies how they handle personal information at each stage of the information cycle, will encourage them to consider how the Privacy Principles apply to their activities.[9]

4.10 The Government outlined the areas where it intended to make amendments to the ALRC's recommendation as follows:

- in order to align the Privacy Principles with the stages of the information handling cycle, the 'openness' principle is to be the first enumerated privacy principle;
- in addition to the obligations proposed by the ALRC, the 'openness' principle should also require entities to take reasonable steps, having regard to the circumstances of the agency or organisation, to develop and implement internal policies and practices that enable compliances with the Privacy Principles including staff training;
- a general obligation to take reasonable steps to implement policies and practices that ensure compliance with the Privacy Principles is to be included in the openness principle in order to ensure a proactive approach to considering information handling and privacy compliance requirements; and
- the obligation to implement policies and practices to enable compliance with the Privacy Principles is to be qualified by a 'reasonable steps' test in recognition that 'the appropriate steps to take will depend upon the circumstances of each agency or organisation' thus adopting a 'risk-based approach'.

4.11 The Government response concluded:

> This additional supporting obligation to the 'openness' principle would expressly recognise what is only implicit in the existing Privacy Principles: that agencies and organisations need to take positive steps to ensure they comply with the Privacy Principles. However, it reflects what many agencies and organisations currently do in practice to ensure they meet their

9 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, p. 48.

> obligations under the Privacy Act. It is therefore not intended to impose any unreasonable additional burden on agencies and organisations.[10]

Issues

4.12 The ALRC, OPC, Privacy NSW and the Australian Institute of Credit Management welcomed the positioning of the openness and transparency principle as the first APP. Professor Rosalind Croucher, President, ALRC, commented further:

> It brings it up to the front as the first principle and provides, as I described it in the submission, a conceptual mirror to the idea of openness that is captured in the freedom of information legislation. That is a good initiative and we commend the introduction of the principles in that fashion.[11]

4.13 Support was expressed for the Government's aim of encouraging entities to manage personal information openly and transparently, as well as the aim of ensuring that entities take reasonable steps to comply with the Privacy Act and to handle complaints. The Government's intention to ensure that entities undertake appropriate planning prior to the point of dealing with personal information, and when planning new information systems, was also welcomed.[12] However, in order to ensure that this was stated more clearly, the NSW Department of Justice and Attorney General suggested that APP 1(2) be re-titled 'Planning for compliance with the Australian Privacy Principles'.[13]

4.14 The committee also received submissions that did not support the notion that the privacy obligations could, or should, be considered when entities design information systems, that is, the 'privacy by design approach'. Microsoft commented that 'it could be hard to read privacy by design elements into the principle as currently worded'. Microsoft went on to state that it would be wary about trying to load this concept into the principle as it is difficult to see how it would be defined or enforced. In addition, it would raise 'real possibilities of inappropriate government interventions into what should properly be business decisions'. Microsoft also pointed to comments by European Union Data Protection Supervisor, Mr Peter Hustinx, who saw privacy by design not as a matter of law, but something that would be achieved through the practices of organisations. Microsoft supported this view and concluded that legislating for privacy by design would be 'onerous, impractical and would have real potential to stifle innovation'.[14]

---

10 Australian Government, *Enhancing National Privacy Protection*, pp 48–50.

11 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 1.

12 Office of the Privacy Commissioner, *Submission 39*, p. 23; Privacy NSW, *Submission 29*, p. 3; Australian Institute of Credit Management, *Submission 8*, p. 2.

13 NSW Department of Justice and Attorney General, *Submission 42*, p. 2.

14 Microsoft, *Submission 14*, p. 9.

4.15 The Office of the Information Commissioner Queensland (OIC) drew attention to the inclusion of a 'reasonable in the circumstances' test in APP 1 and commented that it did not consider that the obligation to comply with the privacy principles should be subject to such a test. The OIC argued that state and territory jurisdictions, which have enacted information privacy laws, impose a mandatory requirement to comply with the relevant privacy principles. In addition, the OIC commented that the adaptable and flexible nature of the APPs provides sufficient scope for entities to implement them in ways which are reasonable, based on the circumstances and context of the entity's personal information handling. As such the OIC recommended that the committee consider APP 1 in terms of whether or not it would be more appropriately stated as a mandatory obligation.[15]

Conclusion

4.16 The committee considers that by placing the 'openness' principle as the first APP, attention is drawn to the need to manage personal information in an open and transparent way. The Government has included in APP 1 an obligation to develop and implement internal policies and practices that enable compliance with the privacy principles. This will strengthen the 'openness' principle and encourage a proactive approach to privacy compliance. The committee believes that by requiring the planning of data systems to take account of privacy requirements, the handling of personal information will be improved and individuals will be confident that entities have taken all necessary steps to provide adequate systems to protect their personal information. Further, the committee does not agree that the 'privacy by design' approach will stifle innovation. Rather, as technology is advancing so rapidly, what is regarded as 'innovation' may in fact pose significant risks to privacy, and thus privacy obligations should be a fundamental consideration in planning information systems.

4.17 The committee also considers that the inclusion of a test of reasonableness ensures that entities have flexibility in the way in which they address the obligations under this principle and, as stated in the Government response, recognises that the appropriate steps to take will depend upon the circumstances of each agency or organisation. In addition, the committee notes that the Government commented in its response to the ALRC's recommendations that:

> In this way, the additional requirement adopts a risk-based approach, whereby an agency or organisation would consider what internal practices and policies to implement with regard to such matters as the volume of personal information it handles, the sensitivity of that information and the purpose for which the information is collected, used and disclosed.
>
> In addition to considering the level of risk in their information handling needs and practices, agencies and organisations would also consider what is reasonable for them to do with regard to their size and available resources,

15 Office of the Information Commissioner Queensland, *Submission 18*, p. 2.

> the type of functions or activities they undertake, and the extent to which they have already established internal policies and practices.[16]

4.18 The committee concurs with this approach.

Structure and terminology

4.19 Submitters commented on the structure of, and the terminology used in, APP 1. The Law Institute of Victoria (LIV) suggested that, to ensure consistency with APP 1(3) which requires an entity to have 'up-to-date policy' on the management of personal information, APP 1(2) should be amended to read 'implement and review practices'.[17]

4.20 The Law Council of Australia (LCA) commented on the terms used in APP 1(2)(a). First, the LCA was concerned about the strength and the mandatory nature of the language used. Secondly, the LCA noted that APP 1(2)(a) requires an entity to take 'such steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure that the entity complies with the Australian Privacy Principles'. The LCA suggested that it is not possible for 'practices, procedures and systems' to ensure compliance with the APPs. In order to address this matter, the LCA suggested replacing the word 'will ensure' with words such as 'have the primary purpose of promoting compliance'.[18]

4.21 The department responded to the LCA's comments and stated that, by including the 'will ensure' formula, the Government has gone further than the ALRC recommendation 'in requiring agencies and organisations not only to create and maintain a privacy policy but to also demonstrate that they have taken reasonable steps to comply with both the privacy principles and their own privacy policy'.

4.22 The department went on to state that the term the 'primary purpose of promoting' provides for a different requirement than the term 'will ensure'. The department argued that the terms of APP 1(2)(a) provide a clear requirement for entities to have practices, procedures and systems that will ensure compliance with the APPs. The term suggested by the LCA was seen as a lesser obligation and 'is not consistent with the Government's approach of promoting high standards of compliance that will require entities to consider how the principles apply to their own circumstances and what steps it should take to implement appropriate policies and practices'. The department concluded that:

> It was the Government's intention for the compliance standards on agencies and organisations to be sufficiently high to enhance privacy protections.

16 Australian Government, *Enhancing National Privacy Protection*, p. 50.

17 Law Institute of Victoria, *Submission 36*, p. 4.

18 Law Council of Australia, *Submission 31*, p. 4.

> The 'will ensure' obligation was included so that privacy protections are built into the design of an entity's system and not 'bolted on' afterwards.[19]

4.23 Microsoft put the view that APP 1(2) is redundant. Microsoft noted that section 16A of the *Privacy Act 1988* provides that 'an organisation must not do an act, or engage in a practice, that breaches a National Privacy Principle'. If, it was argued, a modified version of section 16A is to be enacted to prohibit breaches of the APPs, regulated entities will be required to take steps to comply with the APPs and thus APP 1(2) is redundant. Microsoft concluded:

> If APP [1(2)] was enacted as proposed, it would be possible for an entity to be liable for breaching APP [1(2)] simply because it had not prepared a document that described the procedures it would take with the objective of ensuring compliance with the remainder of the APPs. This would be so even if there had been no breach by the entity of any of the substantive APPs…
>
> We just do not believe that APP [1(2)] will assist individuals whose privacy is at risk of being interfered with - they will have remedies if and when a breach of the substantive principles occurs. In a case involving serious and systematic breaches of the APPs, a court has power under section 98 of the Privacy Act to require an entity to take positive steps to prevent future breaches. This power would likely extend to introducing a compliance program - similar orders are commonly made at the request of the ACCC in cases involving contraventions of the Trade Practices Act.[20]

4.24 The OPC also commented on the complexity of the term 'steps as are reasonable in the circumstance' used in APP 1 and other APPs.[21] The committee has addressed these comments in its discussion on the complexity of the APPs in chapter 3.

Privacy policy requirements

4.25 APP 1 also sets out the requirements for an entity's privacy policy: first, that it must be clearly expressed and up-to-date (APP 1(3)); and secondly, that it must contain certain information (APP 1(4)). These provisions were supported by the Health Services Commissioner, Victoria, who noted that the provisions of APP 1 go further than the existing provisions in the Privacy Act and the equivalent provisions in the Victorian Health Records Act.[22] Similarly, the Office of the Victorian Privacy Commission supported the more prescriptive nature of APP 1 as 'it will better allow individuals to identify precisely how entities intend to handle personal information'.[23]

---

19 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 6.

20 Microsoft, *Submission 14*, p. 9.

21 Office of the Privacy Commissioner, *Submission 39*, p. 23.

22 Health Services Commissioner, Victoria, *Submission 26*, p. 2.

23 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 3

4.26 The committee received comments suggesting improvements to the privacy policy provisions. Professor Graham Greenleaf and Mr Nigel Waters, in their joint submission, commented on the need to make the list of matters to be included in an entity's privacy policy more consistent with the list of matters to be notified when collecting personal information under APP 5. For example, APP 1(4) requires information about how an individual may access information (d) and complain (e), but not 'identity and contact details' (APP 5(2)(a)).[24]

4.27 The NSW Department of Justice and Attorney General suggested that privacy policies should also provide some description of the individuals or entities who are likely to receive personal information and commented that 'this is crucial in terms of giving members of the public a real picture of how personal information is handled and to answer the question: "who are they giving it to?".' It was argued that such a requirement would complement the obligations under the disclosure principle (APP 5(f)).[25]

4.28 Other submitters, however, raised a range of concerns about the prescriptive nature of the information to be included in an entity's privacy policy. For example, the LCA suggested that the privacy policy should only be required to contain 'reasonable information' or 'general information' about the various matters listed.[26]

4.29 The Australian Finance Conference (AFC) also commented that the prescriptive approach was at odds with the objective of providing high level principles and recommended that APP 1(4) be omitted entirely. Both the Australian Association of National Advertisers (AANA) and AFC recommended that the guidance on content of privacy policies be left to the Australian Information Commissioner.[27] Similarly, the AANA submitted that the provisions in relation to privacy policies be limited to core information requirements and that guidance, as is currently the case, be developed to assist entities in meeting their obligations.[28]

4.30 Microsoft's comments concerning APP 1(4) were based on 'evidence that individuals can be overwhelmed but not enlightened by long privacy policies or disclosure statements, even where intended to allow informed consent'. Microsoft submitted that layered privacy notices were one way of improving understanding of privacy policies by providing clear and concise summaries with links to the full privacy statement for those interested in more detailed information. Microsoft suggested APP 1(3)–1(6) (and APP 5) be streamlined by focusing on identifying transparency objectives. Organisations could then choose how best to communicate with individuals to meet these objectives in an effective and cost efficient way.

---

24 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 5.

25 NSW Department of Justice and Attorney General, *Submission 42*, p. 2.

26 Law Council of Australia, *Submission 33*, p. 4.

27 Australian Finance Conference, *Submission 12*, p. 3.

28 Australian Association of National Advertisers, *Submission 21*, p. 6.

Microsoft concluded that 'this would help reduce the compliance burden on organisations and reduce the load on individuals'.[29]

4.31 A range of comments were received in relation to APP 1(4)(g) which requires that if an entity is likely to disclose personal information to overseas recipients, the entity's privacy policy must, if it is practicable to do so, contain the countries in which such recipients are likely to be located. The inclusion of this requirement was supported by Privacy NSW.[30] In addition, Professor Greenleaf and Mr Waters argued that the inclusion of the term 'if it is practicable to specify those countries' provided a far too subjective qualification, and 'is likely to lead to many entities not including this important information'. It was suggested that entities, which do not include this information, be required to give an explanation as to why countries were not specified in the privacy policy.[31]

4.32 Other submitters did not support the inclusion of the obligation under APP 1(4)(g). It was argued that to comply with the obligation was impractical, onerous and costly.[32] Submitters, for example, Yahoo!7 and the Australian Bankers' Association (ABA), commented on the obligations imposed by APP 1(4)(g) for those entities which use overseas servers and cloud computing. It was argued that it was impractical to list all countries, with the ABA noting that banks do not control the location of an overseas server and the server's location may change without the bank's knowledge. The ABA argued that to keep track of these changes, and to continuously update privacy policies, would be onerous and costly.[33]

4.33 The ABA also suggested that APP 1(4)(g) may lead to an individual drawing an incorrect inference that a country named as the location of the intended overseas recipient is not to be trusted with the personal information and 'this would be an unfortunate signal for Australia's law to send internationally'.[34]

4.34 A number of suggestions to address concerns with APP 1(4)(g) were put to the committee. Yahoo!7 favoured a simple disclosure obligation which referred to international data transfer and backup more generally.[35] However, Telstra suggested that the use of very broad references and catch-alls in a privacy notice would diminish

29 Microsoft, *Submission 14*, pp 9–11.

30 Privacy NSW, *Submission 29*, p. 3.

31 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 5; Attachment 1, p. 4.

32 See for example, Australian Bankers' Association, *Submission 15*, p. 3.

33 Australian Bankers' Association, *Submission 15*, p. 3; see also Telstra Corporation Ltd, *Submission 19*, p.1.

34 Australian Bankers' Association, *Submission 15*, p. 3.

35 Yahoo!7, *Submission 20*, p. 1.

the value of providing the information and may lead to confusion. Thus, Telstra argued that APP 1(4)(g) should be omitted.[36]

4.35 The ABA suggested the addition of the words 'reasonable and' before the word 'practicable' to take into account potential volatility in the location of servers in other countries.[37] A number of submitters suggested that as APP 8 deals specifically with cross-border disclosure of personal information APP 1(4)(g) is irrelevant.[38]

4.36 Again, concerns were raised that consumers would not be assisted by long and complex information, specifically in relation to APP 1(4)(f) and (g). Privacy Law Consulting was also of the view that there may be limited benefit to consumers of the provisions as 'they do not result in consumers being provided with a level of information that will enable them to properly consider privacy issues associated with the overseas disclosure'.[39] The AANA also commented that APP 1(4)(f) and (g) 'are unnecessary and not useful information to an individual'. Rather, the AANA submitted that 'the intent of these provisions is to alert individuals that an overseas recipient may not be subject to privacy legislation similar to that of Australia'.[40]

4.37 Privacy Law Consulting voiced concern with the requirement of APP (4)(f) and (g) in relation to the disclosure of commercially confidential information and stated that these obligations may result in the disclosure of details about an organisation's operational arrangements and 'inner-workings'. Privacy Law Consulting gave the example of the outsourcing of back-office functions such as accounts or dictation transcription and noted that such information is not normally made public.[41]

Conclusion

4.38 The committee considers that there are benefits in including in the APPs a list of requirements for privacy policies: it helps to promote transparency; provides consumers with a clear indication of what must be included in a privacy policy; and by having to provide clear privacy policies, entities will be required to examine how they handle personal information at each stage of the information cycle.

4.39 While the committee acknowledges concerns that such an approach may compromise the aim of high-level principles in the Privacy Act and that consumers do not always comprehend overly long privacy policies, the committee considers that the benefits to transparency and overall compliance with the privacy principles outweigh

---

36 Telstra Corporation Ltd, *Submission 19*, p.1.

37 Australian Bankers' Association, *Submission 15*, p. 3.

38 National Australia Bank, *Submission 2*, p. 2; Australian Bankers' Association, *Submission 15*, p. 3.

39 Privacy Law Consulting, *Submission 24*, p. 1.

40 Australian Association of National Advertisers, *Submission 21*, p. 6.

41 Privacy Law Consulting, *Submission 24*, p. 1.

these concerns. The committee considers it is important that the principle provides for the minimum amount of information that is required in a privacy policy and makes it clear that it is not exhaustive and that further information must be included as the particular circumstances of the entity require. On balance, the committee therefore supports the inclusion of the matters to be addressed by a privacy policy within the body of the principle. The committee also notes that the Government encourages the Office of the Australian Information Commissioner to provide guidance in this matter.

4.40 In relation to APP 1(4)(g), the committee considers that many consumers have concerns about the transfer of personal information overseas and that this practice is increasing as technology changes and global markets expand. The committee therefore believes that privacy policies should include information if an entity is likely to disclose personal information to an overseas entity and the countries in which such recipients are likely to be located. The committee notes that APP 1(4)(g) contains the proviso that 'if it is practicable to specify those countries in the privacy policy'. The committee considers that this provides sufficient flexibility to address concerns raised by Yahoo!7 and the Australian Bankers Association.

Availability of privacy policy

4.41 Both the NSW Department of Justice and Attorney General and Professor Greenleaf and Mr Waters commented that the proposal that an entity's privacy policy need only be made available 'in such form as is appropriate' (APP 1(5)(b)) was different to the ALRC's recommendation that access must be provided 'electronically'. Professor Greenleaf and Mr Waters argued that the proposed provision was both weaker and inferior and went on to argue that the requirement in APP 1(6) for entities to respond to an individual's request for the policy in 'a particular form' is only a partial and relatively weak substitute.[42] The NSW Department of Justice and Attorney General commented that:

> In the interests of transparency and accountability, APP1 could explicitly state that entities should take reasonable steps to make the policy available electronically. In practice, this will most likely result in policies being posted on the websites of entities that have them. This is likely to be the first place members of the public will look for privacy policies and it may be appropriate to make explicit the requirement to make them available in this manner.[43]

4.42 The department responded to concerns about APP 1(5) and stated that it believed that an absolute requirement to provide the privacy policy electronically would be a significant burden on organisations without a website or means to otherwise produce an electronic copy. The department went on to state that APP 1(5)(b) puts agencies and organisations under an obligation to provide an appropriate copy of their privacy policy in a way which is reasonable in all the

42 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 6.

43 NSW Department of Justice and Attorney General, *Submission 42*, p. 2.

circumstances, having regard to the agencies' or organisations' functions, types of business and restrictions. It also addresses issues around accessibility; for example, clients of some entities may not have computers and therefore are unable to electronically access privacy policies. The department concluded that, as a consequence, there should be the option available of providing the policy in any other appropriate format.[44]

4.43 Professor Greenleaf and Mr Waters also suggested that it was undesirable for APP 1(6) to apply only to requests from individuals as often organisations such as NGOs and the media may seek access to privacy policies, and this should be expressly accommodated.[45] In response to this suggestion, the department stated the provision is based on ALRC recommendation 24-2, which also uses the terminology 'individual'. While there is no definition for 'individual' in either the APPs or the ALRC Report, paragraph 22(1)(aa) of the Acts Interpretations Act defines an 'individual' as a 'natural person'. The department went on to state that there is nothing preventing an individual within an organisation, or the media, from making the request and concluded:

> Therefore, in practice, there should be no foreseeable problem in media or organisations gaining access to relevant documents containing the Privacy Policies of an agency or organisation.
>
> It is not the Government's intention to prevent organisations from making requests for an entity's privacy policy. Therefore, the Department will consider the Senate Committee's recommendations on this issue, including suggestions for improving clarity on this issue.[46]

Conclusion

4.44 The committee considers the requirement for an entity to make its privacy policy available 'in such form as appropriate' should be further clarified by the inclusion of a note at the end of APP 5 indicating that the form as is appropriate will usually be an online privacy policy. In relation to concerns about access to privacy policies by organisations including the media, the committee does not believe that an entity would deny access through a narrow reading of the provisions of APP 1(6). However, to ensure that the intent of the provision is clear, the committee considers that the provision be re-drafted to clarify that privacy policies must be available to both individuals and entities.

Recommendation 6

4.45 The committee recommends that a note be added at the end of APP 1(5) which indicates that the form of an entity's privacy policy 'as is appropriate' will usually be an online privacy policy.

---

44 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 6.

45 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 6.

46 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 7.

Chapter 5

Australian Privacy Principle 2–anonymity and pseudonymity

Introduction

5.1 Australian Privacy Principle 2 (APP 2) ensures that individuals are permitted to interact with entities while not identifying themselves, or by using a pseudonym. The Companion Guide states that APP 2 emphasises the importance of first considering whether it is necessary to collect personal information at all. By doing so, privacy protection to individuals is improved as it prevents an entity from collecting personal information if it is not needed by the entity. APP 2 recognises that there are some instances where the entity is not necessarily interested in the identity of the individual but rather that the credentials of the individual have been sufficiently established for the purpose of the transaction.

5.2 Entities will only be required to comply with APP 2 where it is lawful to do so. If a law requires the individual to identify him/herself to the entity, then it is not lawful and practicable for them to interact anonymously or pseudonymously.

5.3 The Companion Guide indicates that the Australian Information Commissioner will be 'encouraged to provide guidance on the principle, including on the types of circumstances in which it will not be lawful or practicable to provide this option'.[1]

Background

5.4 National Privacy Principle 8 (NPP 8) requires that private sector organisations provide an opportunity to individuals, where lawful and practicable, to interact on an anonymous basis when a transaction is taking place. The Australian Law Reform Commission (ALRC) stated that 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'. In addition, it allows an individual, where applicable, to provide highly personal or intimate information to an entity with a minimal risk to having their identity traced or revealed.[2]

5.5 There is no comparable anonymity principle in the Information Privacy Principles although the privacy legislation of some state jurisdictions (Victoria,

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, pp 9–10.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 689.

Tasmania and the Northern Territory) contain an anonymity principle that is applicable to public sector bodies.[3]

5.6 Both submitters to the Senate Legal and Constitutional Affairs References Committee 2005 inquiry into the *Privacy Act 1988* and the ALRC review called for the strengthening of the anonymity provisions in privacy legislation.[4]

5.7 In its submission to the Legal and Constitutional Affairs Committee, the Australian Privacy Foundation (APF) commented that the provision had failed to live up to its potential as a significant protection device, due partly to inadequate promotion and enforcement. It was noted that NPP 8 needed to be implemented at the design stage of initiatives so that claims of 'impracticability' could not be used for not offering an anonymous option. The APF also recommended a pseudonymous option as the next best practice where anonymity is either impracticable or unlawful.[5]

5.8 The ALCR review focussed on:

- whether the anonymity principle should be extended to public sector agencies;
- whether pseudonymity should be included in the principle; and
- what should be contained in the model Unified Privacy Principle (UPP).

5.9 The ALRC formed the view that the anonymity principle should be extended to public sector agencies. In coming to this view, the ALRC commented that 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'. In addition, the ALRC argued that an option for dealing with agencies anonymously may potentially give rise to significant public policy benefits, for example, by encouraging individuals to seek medical or other assistance from agencies when they may not have been inclined to do so if they were required to identify themselves.[6]

5.10 The ALRC reported that during its review, the addition of a pseudonymity option was generally supported, particularly in the online environment. The ALRC therefore recommended that the anonymity principle should provide for pseudonymous transactions. The ALRC commented:

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 690.

4 Senate Legal and Constitutional Affairs References Committee, Inquiry into the *Privacy Act 1988,* Electronic Frontiers Australia, *Submission 17,* p. 44; Australian Privacy Foundation, *Submission 32,* p. 17.

5 Senate Legal and Constitutional Affairs References Committee, Inquiry into the *Privacy Act 1988,* Australian Privacy Foundation, *Submission 32,* p. 17.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 693.

> 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.[7]

5.11 The ALRC saw the anonymity option being available in instances where an entity did not need to contact the individual in the future. Where some form of identifier is required, but need not be personal information, pseudonymity is likely to be appropriate.

5.12 The ALRC noted that there was widespread concern about the practical application on the anonymity and pseudonymity principle which ranged from conflict with legislative requirements on an organisation to retain identifying information, to possible misuse of the 'practicable' element to avoid the principle completely.[8] The ALRC was of the view that the best way to address these concerns was to clarify the principle by using 'interacting' with an entity rather than 'transacting' as contained in NPP 8. The ALRC was also of the view that additional certainty was needed for the 'lawful and practicable' requirements.[9]

5.13 It was also the ALRC's view that agencies and organisations need to give a 'clear' option to interact anonymously or pseudonymously as this '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'.[10] The ALRC also stated that the onus should be on agencies and organisation to give individuals options to interact anonymously and pseudonymously.[11]

5.14 In relation to guidance, the ALRC recommended that the Office of the Privacy Commissioner (OPC) should develop and publish guidance on:

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 696.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 696–700.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 700–701.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 705.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 706.

(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.[12]

Government response

5.15 The Government accepted both ALRC recommendations in relation to anonymity and pseudonymity. The Government response stated that anonymity and pseudonymity, limited to where lawful and practicable, are 'an effective way to protect individuals' privacy by ensuring that personal information is only collected where necessary'. In addition, the Government response stated that guidance on the issue will be very important in explaining that the right to interact anonymously or pseudonymously is limited to where it is lawful and practicable in the circumstances. The response also noted that it would be a decision for the Privacy Commissioner to provide guidance.[13]

Issues

5.16 This principle was generally welcomed by submitters.[14] The Office of the Victorian Privacy Commissioner noted the benefits of an individual having the option to interact anonymously or pseudonymously with an entity and stated:

> Where an organisation allows individuals to transact anonymously, the benefits are mutual. The individual transacts without giving up any control over his or her personal information. The entity will not incur any of the obligations that follow from collection of personal information under the other APPs…Providing an anonymity option is also consistent with the principle that an organisation or agency should not collect personal information unless this is necessary for one or more of its functions or activities.[15]

5.17 The Communications Council stated that APP 2 would significantly impact on the way in which entities interact with individuals, particularly in the online

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 708.

13 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, p. 39.

14 See for example, Health Services Commissioner, Victoria, *Submission 26*, p. 2; Privacy NSW, *Submission 29*, p. 3; Internet Society of Australia, *Submission 41*, p. 2.

15 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 3–4.

environment. The Council noted that entities will need to first consider whether it is necessary to collect personal information and 'this is likely to call into review, and ultimately limit, the circumstances in which entities can request personal information from individuals'.[16]

5.18 Abacus Australian Mutuals and the Australian Bankers' Association also supported APP 2 as it was seen as providing greater clarity to financial institutions when they decline customers' requests to undertake transactions anonymously or pseudonymously because of obligations under anti-money laundering and counter terrorism laws.[17] The Internet Society of Australia (isoc-au) commented that increasingly, individuals must complete 'required information fields' on a website before they will be provided with information or before a transaction is finalised. A provision allowing for pseudonymity ensures that transactions can be completed without unnecessary personal information being provided.[18]

Structure and terminology

5.19 In relation to APP 2, Qantas commented that it replaced NPP 8 which, it contended, used much simpler language. Qantas concluded that it was difficult to see why it was necessary to replace NPP 8 when the meaning is unchanged.[19]

Provision of a 'clear option'

5.20 There was concern amongst some submitters that, contrary to the ALRC's recommendation and the Government response, APP 2 did not provide a 'clear option' for individuals to interact anonymously or pseudonymously where it is 'lawful and practicable in the circumstances'.[20] There were two matters raised: first, that APP 2 could be read as only requiring either the option of anonymity or pseudonymity, not both; and secondly, that the exceptions in APP 2(2) could be used to undermine the intent of the principle.

5.21 Submitters commented that APP 2 should be drafted to ensure that both options be available. The NSW Department of Justice and Attorney General stated that clarity could be gained by replacing the term 'or' with the term 'and'. However, it further commented that if one option is not practicable, there could be an exception from the requirements.[21]

---

16 The Communications Council, *Submission 23,* p. 9.

17 Abacus Australian Mutuals, *Submission 7,* p. 1; Australian Bankers' Association, *Submission 15,* p. 4.

18 Internet Society of Australia, *Submission 41,* p. 2.

19 Qantas, *Submission 38,* p. 3.

20 Office of the Privacy Commissioner, *Submission 39,* p. 24.

21 NSW Department of Justice and Attorney General, *Submission 42,* p. 3.

5.22 Professor Graham Greenleaf and Mr Nigel Waters also argued that the wording of APP 2 may allow entities to offer only pseudonymity rather than anonymity or pseudonymity. Professor Greenleaf and Mr Waters submitted an amendment to APP 2 which they considered would overcome these identified weaknesses:

> After APP 2(1) insert:
>
> Where subsection (1) does not apply, an individual must have the option of using a pseudonym unless it is impractical for an entity to deal with individuals who use a pseudonym;[22]

5.23 The exceptions to the principle are provided in APP 2(2). The OPC pointed to the provisions in APP 2(2)(a) that allowed entities not to offer an option if they are 'required or authorised by or under an Australian law, or an order of a court or tribunal, to deal with individuals who have identified themselves'. The OPC argued that as the 'authorisation is not tied to the particular circumstances', it may mean the exception is unnecessarily broad.

5.24 The OPC pointed to the case where an entity may be required to deal with identified individuals only in certain instances and not in others; for example, service delivery agencies which make payments on an identified basis, but may provide other information or services anonymously, including online. The exception under APP 2(2)(a) should only apply to the transaction if there is a legal requirement for identification for that transaction. However, the OPC argued that the wording of draft APP 2 'might be seen as exempting an entity from giving these options if it is "required or authorised" to identify individuals in any context'.[23]

5.25 The OPC put forward three options for consideration by the committee:

a. adopt the phrase 'where lawful and practicable' in APP 2, as in ALRC recommendation 20-1;
b. limit the exception in APP 2(2)(a) to where the legal requirement or authorisation applies in the circumstances of the individual's transaction; or
c. clarify and limit the breadth of the 'required or authorised by law' exception in explanatory material for this principle.

The OPC saw options A and B as being stronger than option C.[24]

5.26 Professor Greenleaf and Mr Waters put a similar view and commented that the re-wording of the exception had weakened the principle as it had moved away from NPP 8's positive formulation of 'wherever…lawful and practicable' and had

22 Professor G Greenleaf & Mr N Waters, *Submission 25*, Attachment 1, p. 3.

23 Office of the Privacy Commissioner, *Submission 39*, p. 24.

24 Office of the Privacy Commissioner, *Submission 39*, p. 25.

made it less clear that the exception applies only to those matters where identification is required by law.[25]

5.27 APP 2(2)(b) provides that if it is impracticable for an entity to deal with an individual who has not identified themselves, the entity need not provide an option of anonymity or pseudonymity. The Law Institute of Victoria (LIV) submitted that this provision is overly broad and may enable entities to circumvent APP 2(1). The isoc-au also argued that the test of 'impracticability' undermined this principle. For example, an entity may argue that it is impractical to change the information fields required for transactions online, but if that information was not reasonably necessary to the information to be provided, or the transaction to be completed, it should not have been required in the first place.[26]

5.28 In order to ensure compliance with APP 2, the LIV recommended that 'impracticable' be defined in guidance notes 'with a view to ensuring that practicability is relevant to the service or goods that the individual seeks to access'. The LIV also suggested that to improve transparency, the privacy policy of entities which wish to rely on APP 2(2)(b), and claim that it is impracticable to deal with individuals who do not identify themselves, address this issue. Alternatively, an entity should make a specific statement to individuals when personal information is sought.[27] The isoc-au recommended that APP 2 be amended so that the exemption to the principle of anonymity and pseudonymity be only allowed if the collection of personal information is reasonably necessary for one of the entity's functions or activities.[28]

5.29 Submitters noted that the ALRC recommended that the OPC provide guidance on the principle and that the Companion Guide stated that the Commissioner will be encouraged to provide guidance, 'including on the types of circumstances in which it will not be lawful or practicable to provide this option'.[29] NSW Department of Justice and Attorney General stated that:

> Guidelines on the circumstances in which compliance is to be considered impracticable under APP2 should set out matters to be considered in deciding whether compliance is practicable. They could make clear, for example, as suggested by the ALRC, that anonymity or pseudonymity generally will not be lawful in the provision of government benefits. It will be important that States are consulted on the content of any such Guidelines.[30]

---

25 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 6; see also Dr Colin Bennett, *Submission 11*, p. 2.

26 Internet Society of Australia, *Submission 41*, p. 3.

27 Law Institute Victoria, *Submission 36*, p. 4.

28 Internet Society of Australia, *Submission 41*, p. 3.

29 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 9–10.

30 NSW Department of Justice and Attorney General, *Submission 42*, p. 3.

5.30 The Department of the Prime Minister and Cabinet (the department) responded to concerns about the provision of a clear option of anonymity and pseudonymity. The department noted that the 'required or authorised' by law exception has been added into every APP. Although the ALRC report did not recommend this exception in relation to the option to interact anonymously or pseudonymously, the department commented that this 'is part of the broader policy of clarifying the operation of that exception'.

5.31 The department also commented on the concern raised by the OPC in relation to the potential for an entity relying on the lawfulness of requiring identification in one instance (for example, providing credit card information for e-commerce purposes), to require the individual to identify themselves when dealing with the entity in another instance. The department stated that 'there is nothing expressly included in the provision to broaden the scope of the exception in that way'.

5.32 The department went on to note that the ALRC examined the existing 'required or authorised by or under law' exceptions in the Privacy Act and noted generally the need for clarity about the meaning of that expression. As a result, the ALRC recommended that the OPC should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. The department concluded that 'although it is a matter for the AIC, the Department believes that the issue raised by the OPC could be included in those guidelines'.[31]

The online environment

5.33 Some submitters commented on the impact of APP 2 in the online environment. Yahoo!7 argued that APP 2 was a 'one size fits all' solution that does not recognise the diverse range of interactions taking place online and that 'context needs to dictate the appropriateness of allowing users to engage anonymously or to interact pseudonymously within these services'. In particular, Yahoo!7 raised concerns about the need to ensure that users are accountable for the use of online services. For this reason, while offering users the ability to interact with other users under a pseudonymous screen name, users are required to register and provide data so that terms of use can be enforced. Yahoo!7 also noted that this data was used by law enforcement agencies when investigating crimes that involve online services.[32]

5.34 In response to Yahoo!7's comments, the department stated it:

> …believes the use of pseudonyms is sufficient to (a) distinguish one individual from another or (b) maintain a transaction history about a person, without retaining a record of their identity. This could be used for agencies or organisations that need this information but do not need to necessarily identify an individual. In developing a framework for the protection of personal information, a key element is whether an agency or organisation

31 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 8.

32 Yahoo!7, *Submission 20*, p. 2.

> needs to collect any personal information (at all) about an individual in order to undertake its functions or interact with the individual. The standard by which agencies or organisations can determine whether personal information is needed should be based on whether it is lawful and practical to interact on an anonymous or pseudonymous basis.
>
> Therefore, if it is unlawful or impracticable for a service provider (such as Yahoo!7) to deal with individuals with anonymity or pseudonymity they would fall under the exception in APP 2(2)(a) and (b). In the cases identified by Yahoo!7 as requiring the collection of identification information (i.e. ecommerce websites authenticating identification for credit card purposes; assisting law enforcement agencies to investigate a crime; registering users for particular core services so that the terms of use of the service can be enforced), the Department's view is that these are likely to come within the exception.[33]

Conclusions

5.35 The committee considers that the provision of the option to deal with entities anonymously and pseudonymously is a positive addition to the privacy regime. However, the committee is concerned that a number of submitters were of the view that APP 2 does not provide a clear option of both anonymous and pseudonymous interactions, unless a listed exception applies; and that the provisions may be broadly interpreted so that an entity can extend the application of the 'required by law' exception inappropriately.

5.36 The committee has considered the department's response to these matters and notes the explanation provided in relation to the 'required by law' exception. However, given the concerns raised by the OPC and other submitters in relation to this exception, the committee believes that further consideration should be given to the wording of APP 2(2)(a) to ensure that the exception cannot be applied inappropriately.

Recommendation 7

5.37 The committee recommends that the wording of APP 2(2)(a) be reconsidered to ensure that the exception to the anonymity and pseudonymity principle cannot be applied inappropriately.

5.38 In relation to comments about the application of APP 2 in the online environment, the committee considers that the provision of options for dealing with entities anonymously and pseudonymously is a positive development. All too frequently it appears that unnecessary personal information is collected in the online environment. The application of these provisions will ensure that entities consider carefully their information requirements when interacting with individuals. The committee further considers that the exceptions provided in APP 2(2) provide entities with sufficient flexibility in this area.

---

33 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 7.

Chapter 6

Australian Privacy Principle 3–collection of solicited personal information

Introduction

6.1 Australian Privacy Principle 3 (APP 3) deals with the collection of solicited personal information including sensitive information. The Companion Guide notes that personal information should only be collected where it is necessary for, or directly related to, one or more of the entity's functions or activities (the functions test). It also provides that an entity must collect information directly from an individual unless it is unreasonable, or impracticable, to do so. If the personal information is sensitive information, the individual must also consent to the collection.[1]

6.2 However, APP 3 provides for a number of exemptions on public interest grounds. These exemptions included exemptions based on National Privacy Principle 10.1 and a number of new provisions. The new provisions reflect the application of this principle to both agencies and organisations.

Background

6.3 Information Privacy Principles (IPPs) 1–3 cover the collection of personal information by agencies. Personal information is not to be collected by agencies unless the purpose is lawful and directly related to the functions or activities of the collector and the collection is necessary. Agencies are to take reasonable steps to ensure that the individual is aware of, among other things, the purpose for which the information is collected and that the information collected is relevant, up-to-date and complete and the collection does not intrude unreasonably on the individual's personal affairs.[2] The IPPs do not regulate the collection of sensitive information separately from other forms of personal information.

6.4 National Privacy Principles (NPPs) provide that an organisation may only collect personal information that is necessary for its functions or activities; and by lawful and fair means. Organisations are to take reasonable steps to ensure that the individual is aware of certain matters including that he or she can access the information. In addition, the collection may be from the individual, if it is reasonable and practicable to do so, or from someone else if reasonable steps are taken to ensure that the individual is aware of certain matters except in the case where making the

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, p. 10.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, pp 710–11.

individual aware would pose a serious threat to anyone's life or health.[3] In relation to sensitive information, the NPPs prohibit the collection of sensitive information except in certain circumstances including that the individual has consented and the collection is required by law. In addition, non-profit organisations are permitted to collect sensitive personal information in certain circumstances.[4]

6.5 The ALRC noted that neither the IPPs nor NPPs require that an individual give his or her consent before an agency or organisation is permitted to collect the individual's personal information.

6.6 The ALRC's review canvassed the issue of collection of personal information directly from an individual, where reasonable and practicable to do so. The ALRC concluded that both agencies and organisations should only collect information from the individual to whom the information relates, where it is reasonable and practicable to do so, and noted that 'such a requirement will increase 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'.[5] The ALRC was of the view that the 'reasonable and practicable' requirement would not limit the coercive information gathering powers of agencies or the exercise of their intelligence, investigative and compliance functions. However, the ALRC recommended that the Office of the Privacy Commissioner (OPC) develop and publish guidance to clarify when it would not be reasonable or practicable to collect personal information only from the individual concerned.[6]

6.7 The ALRC's consideration of the collection of sensitive personal information focused on whether agencies should also be subject to restrictions in collecting sensitive information. The ALRC concluded that there were strong policy reasons to extend restrictions on collection of sensitive information to agencies and noted:

> 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, should allow for the collection of sensitive information by agencies for legitimate reasons.[7]

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 711.

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 735–36.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 718.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 718–19.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 740–41.

6.8 In addition, the ALRC saw no reason for a separate privacy principle to deal with the collection of sensitive information. Rather, it recommended a single principle dealing with the collection of all personal information.[8]

6.9 There are a range of exceptions to the prohibition against the collection of sensitive personal information. The ALRC commented as follows:

- *required or authorised by or under law:* the ALRC concluded that an exception where the collection of sensitive information is required by law is too narrow; rather, the legitimate collection of sensitive information authorised by law should be included in the principle. Concerns that 'specific' authorisation to collect sensitive information is rarely provided for in legislation were acknowledged in the review and it was noted that a review of current legislation may be required to ensure that, where needed, the collection of sensitive information is specifically authorised;[9] and
- *emergency situations:* in emergency situations, where an individual is unable to give consent, the ALRC noted that the Privacy Act contains a separate regime for the collection, use and disclosure of personal information in situations where the Prime Minister or a minister has declared an emergency or disaster. In addition, NPP 10 generally allows for the collection of sensitive information by organisations where it is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual and the individual is incapable of giving consent. The ALRC considered the application of NPP 10 to both agencies and organisations and concluded that it should apply to agencies. However, the ALRC did not support the current requirement of NPP 10 that the threat must be both serious and imminent as it saw this as too difficult to satisfy. The ALRC was of the view that the wording should be relaxed so that it is triggered where the threat is serious, but not necessarily imminent.[10]

6.10 The ALRC also considered other circumstances where exceptions may be warranted; for example, collecting sensitive personal information where essential services are to be provided to individuals incapable of giving consent. The ALRC did not consider that the benefits would outweigh the difficulties of the creation and implementation of such an exception.[11]

---

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 741.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 738–41.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 741–44.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 748–751.

6.11 In relation to the other exceptions currently contained in NPP 10.1, the ALRC commented:

- *consent exception:* NPP 10 allows for sensitive personal information to be collected where the individual has given consent. The ALRC concluded that it is undesirable to amend the consent exception to require express consent for the collection of sensitive information;
- *exception relating to non-profit organisations:* non-profit organisations may collect information in the course of their activities where certain specified conditions are met. The ALRC commented that concerns about the drafting of this exception are best addressed by the Office of the Parliamentary Counsel;
- *exception relating to legal and equitable claims:* collection is permitted where it is necessary for the establishment of, exercise or defence of, a legal or equitable claim. The ALRC was not convinced that there was a need to broaden this exception but did not receive sufficient feedback from stakeholders to make a proper assessment of the merits of broadening the exception. The ALRC did not recommend an amendment to this exception; and
- *exception relating to alternative dispute resolution:* the ALRC was of the view that collecting sensitive information should be permitted where it is necessary for the purpose of confidential alternative dispute resolution.[12]

Government response

6.12 The Government accepted in full all but one of the ALRC's recommendations in relation to collection of sensitive information. The Government accepted in part the ALRC's recommendation that the sensitive information provisions should contain an exception permitting the collection of sensitive information by an entity where it is necessary to lessen or prevent a serious threat to life or health or the individual is legally or physically incapable of giving or communicating consent. The Government response noted that for consistency, a 'serious threat' should refer to 'life, health or safety'.[13]

Issues

6.13 Some submitters expressed their supported for APP 3.[14] However, Professor Graham Greenleaf and Mr Nigel Waters argued that APP 3 is 'significantly weaker

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, pp 752–55.

13 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, p. 44.

14 Office of the Guardian for Children and Young People, *Submission 4*, p. 4; Australian Bankers' Association, *Submission 15*, p. 4; Office of the Health Services Commissioner, *Submission 26*, p. 2.

than the equivalent NPP(1)' and pointed to a number of concerns including the use of the term 'reasonably necessary' rather than 'necessary'.[15] The matters raised by Professor Greenleaf and Mr Waters and other submitters are addressed below.

Structure

6.14 The committee received a range of comments relating to the structure of APP 3. While welcoming the concept of distinguishing between the collection of solicited and collection of unsolicited information, the Australian Institute of Credit Management (AICM) was of the view that the collection of sensitive information should also be placed in a separate principle. The AICM commented that entities did not always recognise information that is necessary to the entity's functions as being 'sensitive information' and that it should be managed with considerable care.[16]

6.15 The OPC also commented on a number of matters related to the structure of APP 3. First, the OPC was of the view that the principle should be titled 'Collection of personal information' and secondly, that the collection of unsolicited information be incorporated into the principle. This latter matter is considered by the committee in chapter 7.

6.16 Secondly, the OPC suggested that APP 3 could be simplified by removing matters which it considered to be repetitious and redundant (APP 3(2)(a)(i)) and consolidating the exceptions as a simpler list under APP 3(2). This would reflect the structure of NPP 10 and the ALRC's model Unified Privacy Principles.[17] Similarly, Professor Greenleaf and Mr Waters suggested consolidation of APP 3(2) and APP 3(3) to simplify the principle.[18]

6.17 Privacy NSW commented that the complex wording of APP 3 'defeats the purpose in choosing principle-based rules rather than legislation' and argued for a more simply expressed principle.[19] Qantas also argued that APP 3 contained 'unnecessary verbiage' with APP 3(2)(a)(i) merely repeating the provisions contained in APP 3(1) while APP 3(5) (third person collection), which replicates NPP 1.4, does so in a less clear and more verbose way.[20]

15 Professor G Greenleaf and Mr N Waters, *Submission 25*, p. 6; see also Australian Privacy Foundation, *Submission 33*, p. 2.

16 Australian Institute of Credit Management, *Submission 8*, p. 2.

17 Office of the Privacy Commissioner, *Submission 39*, p. 27.

18 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

19 Privacy NSW, *Submission 29*, p. 3.

20 Qantas, *Submission 38*, p. 5.

Conclusion

6.18 In chapter 3, the committee has commented on the need to refine the APPs. The committee considers that APP 3 is another example of where simplifying the approach taken would improve the readability of the principle.

Use of the term 'reasonably necessary for, or directly related to'

6.19 The committee received a range of comments in relation to the use of the term 'reasonably necessary for, or directly related to' in APP 3. The AFC supported the inclusion of the term 'reasonably' necessary as reflecting a 'compliance framework that appropriately balances privacy and public interest rights'. However, the AFC did not support the addition of the 'directly' to the 'related to' element as it was argued that this did not appear to be in line with the recommendations of the ALRC. Such wording, it was argued, adds an 'unnecessarily prescriptive aspect to this component of the principle and is at odds with the Government's high-level, non-prescriptive approach and an appropriate balance between the interests of the individual and the public'.[21]

6.20 Other submitters, including Professor Greenleaf and Mr Waters, commented that the proposed wording of APP 3 would result in weaker privacy protections as it was argued that the 'reasonably necessary' test broadened the principle.[22] The Victorian Privacy Commissioner voiced concern about the use of both the terms 'reasonably necessary' and 'directly related to' and commented on the need to ensure that protections were not lowered:

> The APPs should represent the highest standard of privacy protection currently enjoyed in Australia, not the lowest common denominator. Agencies or organisations should only collect personal information that is *necessary* for their functions or activities (as provided by the current VIPP 1.1 in the Information Privacy Act), not information that an agency or organisation reasonably believes may be necessary for their functions or activities, or which is directly related to them.[23]

6.21 One of the weaknesses, it was argued, arises as APP 3(1) 'allows multi-function entities to request personal information that is not directly related to the goods or services actually requested by the individual' as the information may be reasonably necessary for any one of the entity's functions.[24] Dr Colin Bennett was of the same view that the use of 'reasonably necessary' allowed entities to state a very broad set of goals and purposes and thereby allows for any collection of personal

21 Australian Finance Conference, *Submission 12*, p. 4.

22 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 6–7.

23 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 4.

24 Law Institute of Victoria, *Submission 36*, p. 5.

information to be 'reasonably necessary' or 'directly related to' their functions and activities.[25]

6.22 Both the LIV and Dr Bennett noted that the Companion Guide indicates that 'reasonably necessary' means that 'from the perspective of a reasonable person the function or activity is legitimate for that type of entity', and is intended to be interpreted objectively and in a practical way. However, Dr Bennett argued that the proposed drafting of APP 3 does not make this clear.[26] The LIV stated APP 3 focuses only on the entity's functions and not on the individual's reasons for disclosing personal information or dealing with the entity.[27] Professor Greenleaf and Mr Waters also commented that the test should be 'the reasonableness of the purpose' rather than merely the reasonableness of information collection in the context of the entity's functions or activities.[28]

6.23 The LIV recommended that the wording be amended to include 'reasonably necessary for the function or activity in which the person is engaging'.[29] Professor Greenleaf and Mr Waters suggested that 'necessary' alone or preferably 'necessary *and* directly related to' the entity's functions or activities would strengthen APP 3.[30]

6.24 The OPC noted that the Government had accepted the ALRC's recommendation on 'collection' and it had stated that 'necessary' should be interpreted objectively and in a practical sense.[31] The OPC considered that, in line with the Government response, and the ALRC's recommendation, the phrase 'necessary for one or more of the entity's functions or activities' was sufficient for all entities under a single set of principles. However, APP 3 includes the 'directly related to' alternative. The OPC argued that this is unnecessary for agencies as often agency functions and activities are tied to enabling legislation, object clauses or related instruments and are thus more easily defined. The OPC concluded that it was not aware of examples where the 'necessary' requirement would prevent an agency from collecting personal information to pursue legitimate functions or activities.

6.25 In relation to organisations, the OPC was of the view that the wording of APP 3 appears to lower the existing NPP standard for organisations, including when collecting sensitive information. The OPC was concerned that uncertainty had been introduced and that this would allow a broader range of personal information to be collected, including sensitive personal information. The OPC concluded that this 'could be inconsistent with the intent of enhanced, not diminished, privacy protections'

---

25 Dr Colin Bennett, *Submission 11*, p. 2.

26 Dr Colin Bennett, *Submission 11*, p. 2.

27 Law Institute of Victoria, *Submission 36*, p. 5.

28 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 6–7.

29 Law Institute of Victoria, *Submission 36*, p. 5.

30 See also Dr Colin Bennett, *Submission 11*, p. 2.

31 Government Response, p. 42.

and recommended that, to maintain the current level of protection in NPP 1, the words 'or directly related to' be removed from APP 3(1) and corresponding provisions.[32]

6.26 Privacy Law Consulting provided a further view in relation to the interpretation of APP 3 contained in the Companion Guide.[33] Privacy Law Consulting suggested that the interpretation provided does not appear to be consistent with the literal reading of APP 3 and continued:

> The interpretation referred to in the Companion Guide would result in the Privacy Act effectively regulating, and limiting, the types of functions and activities an entity could perform or engage in (based on a test relating to whether they were reasonably legitimate for that type of entity). Such an outcome appears to be beyond the intended scope and purpose of the Act. Further, this would be inconsistent with the general demise of the doctrine of ultra vires in respect of corporations (which placed limitations on activities a corporation could engage in based on its objects clause in its memorandum of association) – see, for example, s 124(1) of the *Corporations Act 2001* (Cth) which generally provides that companies have the legal capacity and powers of an individual, effectively abolishing the application of the doctrine in relation to corporations established under that Act.
>
> It is important that any uncertainty in this regard be eliminated, otherwise entities operate under the spectre that functions or activities they perform or engage in could be challenged on privacy grounds.[34]

6.27 At the committee's hearing on the exposure draft, Professor Rosalind Croucher, President, ALRC was asked to respond to concerns about the possible weakening of the collection principle under proposed APP 3.[35] In a written response, Professor Croucher stated that the UPP recommended by the ALRC followed NPP 1.1 rather than IPP 1.1 as the ALRC was of the view that the NPPs should form the general template for the drafting and structuring of the new unified principles.

6.28 Professor Croucher went on to state that 'it is not entirely clear whether the formulation in APP 3(1) provides more or less privacy protection than that in NPP 1.1' and commented:

> Arguably, allowing the collection of information where it is "directly related" to a function or activity, as well as where it is "necessary", broadens the scope for collection. However, as discussed in ALRC Report 108, the Office of the Privacy Commissioner's 2001 guidelines on collection of information by organisations provide that:

---

32 Office of the Privacy Commissioner, *Submission 39*, p. 26.

33 Privacy Law Consulting, *Submission 24*, p. 2.

34 Privacy Law Consulting, *Submission 24*, p. 2.

35 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 7.

> The Commissioner interprets "necessary" in a practical sense. If an organisation cannot in practice effectively pursue a legitimate function or activity without collecting personal information, then the Commissioner would ordinarily consider it necessary for that function or activity. (p 27)

Further, the High Court of Australia has noted that there is 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' (see *Mulholland v Australian Electoral Commission* (2004) 220 CLR 181, [39].

It should also be observed that, arguably, APP 3 is more privacy protective than NPP 1 in that it requires that collection is 'reasonably' necessary. The addition of this objective element was an option considered, but rejected as unnecessary, in ALRC Report 108, [21.77].[36]

6.29 The Department of the Prime Minister and Cabinet (the department) also provided answers to questions on notice in relation to APP 3. The department commented that the wording in APP 3(1) is intended to strike the appropriate balance between the need to protect against the unnecessary collection of personal information and the need for organisations and agencies to collect personal information reasonably necessary for, or directly related to, one or more of the their functions or activities.

6.30 The department explained the basis of APP 3 as follows. There are two key elements to APP 3(1): first, a 'reasonably necessary' test is included in relation to the collection of 'personal information other than sensitive information'. This is consistent with the views of the ALRC that an objective test should continue to apply as is currently the case for organisations under NPP 1 (although the ALRC believed that an objective test was implied even with the use of only 'necessary'). The department argued that the requirement on entities to collect only personal information that is reasonably necessary to their functions, requires the collection of personal information to be justifiable on objective grounds, rather than on the subjective views of the entity itself. The department concluded that this will limit inappropriate collection by entities.

6.31 Secondly, the term 'directly related to' one or more of the entity's functions or activities ensures that there must be a clear connection between the collection and the entity's functions or activities. The department commented that that aspect of the test appears in the existing IPPs, which bind agencies. The department also noted that IPP 1 has operated under the existing regime in circumstances where it may not be possible to meet the 'reasonably necessary' test. This element is being retained because there may be agencies (less so for organisations) that need to collect personal information to effectively carry out defined functions or activities but who may not meet an objective 'reasonably necessary' test.[37]

---

36 Australian Law Reform Commission, *Answers to Question on Notice,* pp 1–2.

37 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice,* p. 9.

Conclusion

6.32 The committee agrees that an objective test is a necessary element in the collection principle. However, given the comments in relation to the addition of the word 'reasonably' in the 'necessary' test, the committee remains to be persuaded that this provides a higher, or even the same, level of privacy protection as the wording of NPP 1.

6.33 In relation to the 'directly related to' test, the committee notes the department's comments that this test appears in the IPPs as there are circumstances where an agency may not meet the 'reasonably necessary' test. The department goes on to comment that this is less of an occurrence for organisations. The committee has taken note of the comments in relation to the potential for organisations to use this test to establish a very broad set of activities and functions on which to base the collection of personal information and at the same time comply with APP 3.

6.34 The committee considers that APP 3 is a less than elegant solution to the drafting of a unified collection principle, and may, in effect, lower privacy protections by allowing organisations to take advantage of a provision which is more appropriately applied to agencies. The committee considers that the 'reasonably necessary' test provides organisations with sufficient flexibility, and is, in fact, substantially similar to what is now provided in NPP 1. The committee therefore does not support the extension of the 'directly related to' test to organisations and recommends that APP 3 should be reconsidered.

Recommendation 8

6.35 The committee recommends that in relation to the collection of solicited information principle (APP 3), further consideration be given to:

- **whether the addition of the word 'reasonably' in the 'necessary' test weakens the principle; and**
- **excluding organisations from the application of the 'directly related to' test to ensure that privacy protections are not compromised.**

Consent

6.36 The committee received comments regarding the consent requirements of APP 3 in relation to sensitive information. APP 3(2) requires that an entity must not collect sensitive information unless the individual consents or the collection falls within an exception listed in APP 3(3). The general issue of consent has been discussed in chapter 3.

Sensitive information

6.37 Generally, the collection of sensitive information should not occur unless the collection meets the functions test and the individual has consented (APP 3(2)). However, there are a number of specific exemptions which allow collection of sensitive information without consent (APP 3(3)).

6.38 The OPC's comments in relation to the collection of sensitive information went to the use of the 'directly related to' test. The OPC was of the opinion that collecting sensitive information should be 'necessary' not 'directly related to' the functions or activities of an agency or organisation. The OPC commented that the drafting of APP 3(2) 'appears to mean that if an exception in APP 3(3) applies, sensitive information may be collected even if it is not 'reasonably necessary for' or 'directly related to' the entity's functions or activities'. As a consequence, APP 3 provides for a lower threshold for the collection of sensitive personal information than does the existing NPP 1. The OPC concluded:

> If the collection of sensitive information is not subject to the same basic test of "necessity" as other personal information in APP 3(1), this is inconsistent with the accepted view that sensitive information should be accorded higher protection.[38]

6.39 The department agreed with the OPC's interpretation that 'sensitive information' could be acquired using an exception in APP 3(3) without the information first needing to be 'reasonably necessary' or 'directly related to' an activity or function of the entity. However, the department pointed out that these exceptions are based on circumstances where there is an overriding public interest in collecting the information and that safeguards have been built into most of the exceptions. The department stated that the safeguards will ensure that, even where there are specific special circumstances, there is still a requirement that collection be based on an objective element (either relating to reasonable necessity or reasonable belief of necessity).[39]

6.40 Submitters also provided a range views on the individual exceptions provided for in APP 3(3). Professor Greenleaf and Mr Waters, for example, argued that the exceptions had been 'dramatically expanded' citing in particular the 'required by law' and 'emergencies' exceptions.[40] Other submitters provided comment on specific exceptions.

Required or authorised by or under Australian law

6.41 APP 3(3)(a) provides an exception in the case of the collection of sensitive personal information that 'is required or authorised by or under an Australian law, or an order of a court or tribunal'. The Victorian Privacy Commissioner voiced concern about this exception, noting that it is similar, but not as stringent, as that contained in the Victorian privacy legislation. The Commissioner stated that the APPs should represent the highest level of current privacy protection in Australia. The Commissioner supported a narrower drafting of the requirement so that an exception

38 Office of the Privacy Commissioner, *Submission 39*, p. 27.

39 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 10.

40 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

is only permissible when the requirement to collect sensitive information is mandatory, and not simply permissive or discretionary.[41]

6.42 Professor Greenleaf and Mr Waters commented that no justification had been provided as to why the 'deliberately more protective wording' of NPP 10 has been abandoned. While accepting that "specifically authorised" may be an appropriate change to this requirement, they did not support 'the wholesale invocation of the very vague and subjective "authorised"'.[42]

Emergencies

6.43 An exception is provided for when an entity believes the collection is necessary to 'lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety' and it is unreasonable or impracticable to obtain the consent of the affected person (APP 3(3)(b)).

6.44 This exception was criticised by Professor Greenleaf and Mr Waters as it was argued that it had been broadened by the removal of the 'imminent' threat criteria. They submitted that it is 'essential to retain a test of "urgency" to justify why another basis for [collection] cannot be established'. In addition, they stated that the exception has also been broadened by the addition of threats to an individual's 'safety' and to 'public health or safety' and by the replacement of the condition that consent be physically or legally impracticable with a much weaker 'unreasonable or impracticable to obtain consent'. Professor Greenleaf and Mr Waters commented that the last change 'is a major weakening of the principle and will be interpreted by entities to routinely justify collection of sensitive information without consent'.[43]

6.45 The Public Interest Advocacy Centre (PIAC) also commented on the absence of the requirement that the threat be 'imminent'. PIAC argued that there must be some degree of urgency and, as a result of that urgency, limited access to other mechanisms available to prevent the threat eventuating. PIAC was of the view that the requirement of imminence acted as an important safeguard, particularly when information was being sought about persons with mental illness. In this case, there may be a potential for serious threat to health, but no imminence, because at the relevant time the illness is well controlled by medication or is episodic and the person is currently not unwell. PIAC concluded that where the threat is serious, but not imminent, other mechanisms should be used to avoid the threat eventuating without recourse to non-consensual collection of sensitive information.[44]

6.46 Qantas, however, argued that the reference to 'serious' should be removed as the question of seriousness is subjective and it 'believed that employees should not be

---

41 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 5.

42 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

43 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

44 Public Interest Advocacy Centre, *Submission 32, Attachment 1*, p. 8.

placed in the position of having to make such a judgment if they reasonably believe that a serious threat exists and it will be unreasonable and impractical to obtain consent'.[45]

6.47 The department provided the following information in relation to the emergencies exception. The ALRC Report stated that the current requirement that a threat must be both serious and imminent in these provisions is too difficult to satisfy, sets a 'disproportionately high bar' and can lead to personal information not being used or disclosed in circumstances where there are compelling reasons justifying its use or disclosure. The removal of 'imminent' would also allow an agency or organisation to take preventative action to stop a threat from developing into a crisis.

6.48 The ALRC's view was accepted by the Government. The department noted that, to address concerns of a number of stakeholders that the removal of this element would inappropriately broaden the exception, a requirement was included that use and disclosure could occur only after consent has first been sought, where to do so is reasonable and practicable. Thus, the additional elements to the exception where 'it is unreasonable or impracticable to obtain the affected individual's consent' to either the collection of sensitive information, or the use or disclosure of personal information.[46]

Unlawful activity

6.49 It was noted that the exception relating to the investigation of unlawful activity was not included in the ALRC's recommendations. Professor Greenleaf and Mr Waters commented that there needs to be some justification for this exception and that it should be qualified on the condition that the entity must take some appropriate action within a reasonable period of time. It was argued that 'without such a condition, the exception invites the compilation and indefinite maintenance of "blacklists" based on suspicion of wrongdoing but without any requirement for individuals on such lists to be afforded natural justice'.[47]

Missing persons

6.50 An exception (APP 3(3)(g)) is available to assist in the location of missing persons. Collection of the information must comply with the Australian Privacy Rules. Professor Greenleaf and Mr Waters argued that, if there is a case for a separate exception for missing persons, the provisions should be contained in the APP and not in the, as yet unknown, Australian Privacy Rule.[48]

6.51 The ALRC did not support the creation of an express exception for disclosing information to assist in missing persons investigations as other exceptions would

45 Qantas, *Submission 38*, pp 4–5.

46 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 10.

47 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

48 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 8.

assist in broadening the scope of situations in which disclosure of personal information in missing persons investigations would be authorised, such as the serious threat exception. The department noted that the Government agreed with the ALRC's view that using or disclosing personal information to locate missing persons may often be permitted by other exceptions. However, the Government considered that 'an express exception should also apply for those instances where the application of other exceptions is unclear'. For example, some agencies were concerned that the 'serious threat to life' etc exception would not allow them to collect information relating to a missing person who may have gone missing because of health issues. The department went on to state that, in order to provide safeguards against improper use of such information, the Government decided that such collection, uses or disclosures should be in accordance with binding rules issued by the Australian Information Commissioner. These are to be in the form of a legislative instrument and therefore subject to the scrutiny of Parliament.[49]

6.52 The department provided further information about the rules and commented that they will consist of detailed matters relating to the procedures and protocols used by agencies that are more appropriately dealt with in subordinate legislation. The department noted that using rules, rather than the Act, will allow a more flexible response to the wide variety of circumstances in which this issue may arise (e.g. natural disasters, child abductions). Further, there is already an example of a non-legislative determination (Public Interest Determination 7) where the Privacy Commissioner has granted a waiver from compliance with IPP 11.1 which permits the Department of Foreign Affairs and Trade to disclose personal information of Australians overseas to their next of kin in certain limited circumstances. The rules will also be subject to extensive consultation and to parliamentary scrutiny.

6.53 The department noted that the Government response provides a non-exhaustive list of matters which may be included in the rules.[50]

Exceptions related to Commonwealth agencies

6.54 There are a number of exceptions (APP 3(3)(e) and (f)) which apply only to Commonwealth agencies; for example, the Defence Force. The Victorian Privacy Commissioner commented that this was problematic when expressly included in the APP itself, as this reduces the simplicity, lucidity and 'high-level' nature of the APPs. In addition, the Commissioner stated that it would reduce the ability of states and territories to readily adopt them with minimal amendment.[51]

6.55 Professor Greenleaf and Mr Waters saw these special exceptions as allowing the Defence Forces and diplomatic service 'to avoid the principle [on] the basis of their own "reasonable belief".' They argued that this reflected 'a lazy approach to

49 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 11.

50 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 12.

51 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 5.

compliance' and that these entities should have to comply with APP 3 and take advantage of the generic exceptions where appropriate.[52]

6.56 The OPC's comments on the inclusion of agency specific exceptions in the APPs are provided in chapter 3.

Implied consent

6.57 Qantas submitted that it often collected sensitive personal information provided by a third party where it is impracticable to obtain consent from the individual about whom it is given; for example, in the case of a carer providing health information while making a booking for the person in their care. Qantas submitted that in these circumstances the consent exception should be expanded to include the situation where consent can be reasonably be inferred from the circumstances of the collection.[53]

Health information

6.58 The NSW Department of Justice and Attorney General raised the concern that APP 3 did not allow for the collection of sensitive health information such as where in providing care for a patient, a family history is taken. It was argued that a health practitioner will not have the patient's family member's consent and in most circumstances, the information collected about the patient's family members will not be necessary to lessen or prevent a serious threat to life, health or safety. The NSW Department of Justice and Attorney General concluded:

> It is imperative that health practitioners can continue to take a patient's family history without having to seek the consent of each family member to collect health information about that family member. APP3 should be amended to allow this to occur.[54]

Conclusion

6.59 The committee notes that the exceptions provided for in APP 3 are 'based on circumstances where there is an overriding public interest in collecting information'. To ensure that these provisions are not abused, safeguards have been incorporated into the exceptions. In particular the committee notes that, in relation to the missing persons exception, Australian Privacy Rules will provide for detailed matters relating to procedures and protocols. The committee considers that this is an appropriate exception to deal with the sometimes very difficult circumstances of missing persons. The use of rules, rather than a non-legislative determination by the Privacy Commissioner, provides for consultation and the scrutiny of Parliament. The committee welcomes this approach.

---

52 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

53 Qantas, *Submission 38*, p. 5.

54 NSW Department of Justice and Attorney General, *Submission 42*, p. 5.

6.60 In relation to the inclusion of agency specific exceptions, the committee has commented on this matter in chapter 3.

Means of collection

6.61 APP 3(5) provides that entities must collect information only by lawful and fair means and the entity must collect the information from the individual concerned. Two exceptions are provided for. The first, APP 3(5)(a), allows agencies to collect information about a person from a third party if required or authorised by or under an Australian law, or by a court or tribunal. The second, APP 3(5)(b), applies where it is 'unreasonable or impracticable' for an entity to collect the information from the individual.

6.62 The Victorian Privacy Commissioner strongly supported the provisions in relation to the direct collection of information from an individual and noted that it enables individuals to have some measure of control over what is collected, by whom and for what purposes as well as allowing individuals to refuse to participate in the collection.[55] The inclusion of the 'reasonable and practicable' requirement was also supported by the Victorian Privacy Commissioner as it allows for circumstances where it may not be practically possible to collect information directly from an individual. However, the Commissioner and the LIV saw the need for guidance as to the circumstances where it would not be reasonable or practicable to collect information directly from an individual. This should be jointly prepared by all Privacy (or Information) Commissioners across jurisdictions.[56]

6.63 The LIV also noted that APP 3(5)(b) does not expressly restrict an entity from on-selling to a third party entity personal information obtained from an individual if it is 'unreasonable or impracticable' for the third party to collect the information from an individual. For example, the third party entity may mount an argument that it was 'unreasonable or impracticable' to collect the information from the individual because of lack of time. The LIV expressed concern that individuals may not have control over where information about them goes, or is used, and recommended guidance on the circumstances in which collection from an individual is deemed to be 'unreasonable or impracticable'.[57]

Collection from third parties

6.64 The restriction to agencies of the collection of information from a third party, if required or authorised by or under an Australian law, was questioned by the ACF. It commented that it 'was not aware of any policy justification for confining the permitted means to collection to include third parties to the public sector' and that this

55 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 5.

56 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 6.

57 Law Institute of Victoria, *Submission 36*, p. 5.

could equally be relevant to the private sector.[58] The Australian Bankers' Association also supported this recommendation as there is increased use of third party verification methods to satisfy legislative requirements, such as anti-money laundering and counter terrorism legislation as well as instances where a third party is required to translate for non-English speaking customers. The ABA recommended that the APP be amended to allow for sensitive information to be collected from a third party where consent has been given.[59]

6.65 The NSW Department of Justice and Attorney General also commented on the collection of information from third persons. It pointed to the NSW Law Reform Commission's recommendation that an entity should be able to collect personal information about an individual from a third person if the individual consents. The basis of this recommendation was that it gives autonomy to the individual about how their personal information may be collected; for example, the person may find it more convenient to allow the information to be collected from a third party. In addition, the NSW Department of Justice and Attorney General pointed to the circumstances facing some agencies. For example, the NSW Department of Housing may need to collect information from a medical practitioner about the mental health of an applicant for priority housing. It is possible that in such a case, it might not be unreasonable or impracticable to obtain the information from the individual in question. Thus, as presently drafted, APP 3 might not authorise the Department to obtain such information from the medical practitioner.

6.66 The NSW Department of Justice and Attorney General noted the comments of the ALRC in relation to this matter: that if personal information is collected from a third person with their consent, individuals will not have the opportunity to refuse to provide information and there is a risk that third parties will not be able to provide up-to-date, complete or accurate information. However, the NSW Department of Justice and Attorney General commented that if a 'consent' exception was considered, it may be appropriate that it relied on 'express' consent. It was concluded that:

> While there are some risks in relation to the nature of the consent and the accuracy and completeness of the information, individuals should be free to choose to have their information collected from third parties where they do not wish to provide the information themselves.[60]

6.67 The department responded to issues raised in relation to 'means of collection', in particular, collection from third parties. The department commented that the exception in APP3(5)(a) was included to address agency concerns that they may be in breach of the Privacy Act where another law allows or requires them to collect from a number of sources other than the individual, but in the circumstances it would still be practicable and reasonable to go to the individual. For example, the Australian

---

58 Australian Finance Conference, *Submission 12*, p. 4.

59 Australian Bankers' Association, *Submission 15*, p. 4.

60 NSW Department of Justice and Attorney General, *Submission 42*, p. 5.

Electoral Commission obtains information from Commonwealth agencies and updates the electoral roll using that information.[61]

6.68 The department went on to explain that currently, NPP 1 allows organisations, where reasonable and practicable, to collect personal information about an individual *only* from that individual. The ALRC did not recommend any change to this. In relation to the concerns raised by the ABA, the department commented that when an entity collects information from a third party for identity verification purposes in accordance with legislative requirements under anti-money laundering and counter terrorism legislation, because it had a suspicion that the person is not who they claim to be, it is likely to be "unreasonable or impracticable" to collect it from the individual concerned. The department concluded that the alternative second element of the exception would apply to allow the collection.[62]

Conclusion

6.69 The committee is of the view that the inclusion of the 'unreasonable and impractical' provision in APP 3(5)(b) provides appropriate flexibility to organisations and therefore there is no need to extend APP 3(5)(a) to organisations.

6.70 The committee has noted the comments of The NSW Department of Justice and Attorney General in relation to the collection of personal information about an individual from a third party when that individual consents to that process. The committee considers that, at the present time, it appears that the risks to privacy outweigh potential benefits.

61 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 12.

62 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, pp 12–13.

Chapter 7

Australian Privacy Principle 4–receiving unsolicited personal information

Introduction

7.1 Australian Privacy Principle 4 (APP 4) ensures that personal information that is received by an entity is still afforded privacy protection, even where the entity has done nothing to solicit the information. When unsolicited personal information is received, an entity must, as a first step, decide whether it could have collected the information in accordance with APP 3. If this is the case, then the other Australian Privacy Principles apply to that personal information in the same way as if it had been solicited. If the entity would not have been permitted to collect the personal information under APP 3, then it must take steps to destroy the information or ensure that it is no longer personal information; for example, de-identify the information.[1]

Background

7.2 The ALRC noted that the Information Privacy Principles (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. IPP 1 does not specifically refer to unsolicited information; however, it has been said to apply to unsolicited information. NPP 1 does not distinguish between the obligations imposed on organisations in respect of solicited or unsolicited information although it does address separately personal information obtained directly from the individual and from a third party.[2]

7.3 The ALRC also noted that many agencies and organisations receive large amounts of unsolicited personal information and commented that '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'. The ALRC saw a risk to a person's privacy arising when entities retain unsolicited information and was of the view that if this occurred, then the entity should comply with the privacy principles in respect of that information.[3]

7.4 When considering the implications of the requirement to comply with the privacy principles in respect of unsolicited information, the ALRC noted that some stakeholders had expressed concern that they would not always be able to comply

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, p. 10.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 720.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 725.

with the obligations imposed by the privacy principles in respect of certain information; for example, the 'Notification' principle. However, the ALRC commented that in some circumstances it will be reasonable for entities to take no steps to notify an individual about collection.

7.5 The ALRC also considered the destruction of unsolicited personal information and came to the conclusion that an obligation to immediately destroy such information was impractical. Rather an entity requires time to consider whether it can lawfully collect the unsolicited information and whether it wishes to retain the information. If there is an affirmative outcome to both these matters, then the obligations that apply to the 'active' collection of personal information should apply. If it is not the case, then the entity should destroy the information as soon as practicable without using or disclosing it—if it is lawful and reasonable to do so.

7.6 The ALRC concluded that this 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.[4]

7.7 The ALRC also recommended that the Office of the Privacy Commissioner (OPC) should develop and publish guidance about the meaning of 'unsolicited' in the context of the 'Collection' principle.

Government response

7.8 The Government accepted the ALRC's recommendations in relation to unsolicited personal information and noted that such information should be afforded privacy protections. Unsolicited personal information that is not necessary for an entity's functions or activities should be destroyed or de-identified, where lawful and practicable to do so, and this should apply if the information is received either from the individual themselves or from any other third party. The Government also accepted the ALRC's recommendation in relation to guidance from the OPC and noted that:

> …it would be important for such guidance to explain how this principle may apply to unsolicited personal information that is necessary for

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 725–26.

compliance, enforcement and regulatory functions, including where confidential "tip-offs" are received.[5]

Issues

Structure

7.9 Some submitters supported APP 4 as it was seen to clarify how an entity should address the management of unsolicited personal information.[6] However, a number of submitters argued that the inclusion of a separate privacy principle dealing with unsolicited personal information was unnecessary and added complexity to the legislation.[7] Qantas, for example, stated that the distinction between 'solicited' and 'unsolicited' personal information has resulted in a much more verbose principle than NPP 1 and 'the proposed new principles [APP 3 and APP 4] are difficult to interpret and the distinction appears to be unnecessary and artificial'.[8] The OPC also suggested that the receipt of unsolicited personal information should be addressed within APP 3, rather than as a separate dedicated principle, as the general collection principle is the logical location for the provision relating to unsolicited information.[9]

7.10 Other submitters, for example, the National Australia Bank, noted that APP 3 already protects against the inappropriate collection of any personal information by the overriding obligation not to collect personal information unless it is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.[10] Similarly, Telstra argued that APP 4 did not afford any additional protections and was unnecessary as APP 11 requires that an entity should destroy any personal information that is no longer required for the purposes permitted by the APPs.[11]

7.11 The Australian Finance Conference (AFC) was of the view that APP 4 'is not necessary and potentially devalues the Government's reform objective'. The AFC noted that APP 4 appears to reflect the intent of the ALRC recommendation that personal information received by an entity, even if not solicited, should still be

---

5 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, p. 41.

6 Office of the Guardian for Children and Young People, *Submission 4*, p. 4; Victorian Privacy Commissioner, *Submission 5*, p. 6; Australian Institute of Credit Management, *Submission 8*, p. 3; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 9.

7 National Australia Bank, *Submission 2;* Australian Finance Conference, *Submission 12*, p. 4; Australian Bankers' Association, *Submission* 15, p. 5; Telstra, *Submission* 19, p. 1; Qantas, *Submission 38*, p. 5.

8 Qantas, *Submission 38*, p. 5.

9 Office of the Privacy Commissioner, *Submission 39*, p. 30.

10 National Australia Bank, *Submission 2*, p. 3

11 Telstra, *Submission 19*, p. 2.

afforded privacy protections and encourage the entity to collect that information directly from the individual where reasonable. However, the AFC argued that draft APP 4 'requires a sophisticated compliance approach that is, in our view, unwarranted' and that the ALRC's Unified Privacy Principle 2.4 would achieve the same result 'with minimal compliance process and consequently cost'.[12]

7.12 The Office of the Information Commissioner, Queensland (OIC) recommended that if it is determined that the unsolicited information could have been collected under APP 3, words should be added to APP 4 that clearly require personal information which is not destroyed or de-identified under APP 4(4) to be managed in accordance with APPs 6 through 13.[13]

7.13 The Department of the Prime Minister and Cabinet (the department) responded to these comments and stated that the insertion of a separate APP covering the collection of unsolicited information is aimed at clarifying the application of the principles explicitly in relation to unsolicited information, rather than implicitly as currently occurs with the NPPs. It also confirms that, where an entity could have collected the unsolicited information, it should be treated in accordance with all the privacy principles that apply to the collection of solicited information. As to the OPC's comments about the location of the requirement, the department stated that 'it is an important standalone principle of collection that should be included in a separate principle'.[14]

Compliance burden

7.14 Submitters also raised concerns that entities would face an increased compliance burden. The Australian Bankers' Association (ABA) commented that additional training of staff would be required 'to recognise that the receipt of certain information may require the determination to be made as required under APP 4', and this will be a very significant practical exercise. The ABA concluded that there would be no clear benefit to privacy principles arising from that additional burden.[15] Telstra also commented on the compliance burden and stated that entities would have to take steps to identify and distinguish between solicited and unsolicited information. This, Telstra suggested, would shift the emphasis away from whether the information in the entity's possession, however collected, is necessary and relevant for its purposes.[16]

7.15 Westpac and Abacus Australian Mutuals provided an example of the practical difficulties with this APP: if both solicited and unsolicited information are provided during a phone call, it may be extremely difficult to extract only the solicited

12 Australian Finance Conference, *Submission 12*, pp 4–5.

13 Office of the Information Commissioner, Queensland, *Submission 18*, p. 5.

14 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 13.

15 Australian Bankers' Association, *Submission 15*, p. 4; see also Telstra, *Submission* 19, p. 2.

16 Telstra, *Submission 19*, p. 2.

information. Abacus Australian Mutuals suggested that the record of the whole phone call may need to be destroyed if the entity is unable to separate the non-required information from the required information. Westpac commented that in such circumstances the entity would have to rely on the separation activity being not 'reasonable' (APP 4(4)). Given the 'risk' of this approach, Westpac recommended that the principle be amended to focus on the subsequent 'use' of such information.[17]

7.16 Abacus Australian Mutuals suggested another option: that APP 4 be re-worded so that if information can't reasonably be disposed of, steps must be taken to ensure it is not used, thereby achieving the same result for the customer.[18]

7.17 Yahoo!7 also pointed to a practical difficulty arising from APP 4 in the case where personal information is provided to another entity and that entity 'cannot secure the same consents as were provided to the original collector but has nevertheless obtained the information in a lawful and privacy abiding manner'.[19] Telstra also commented on such instances and stated that an alternative function for APP 4 would be to:

> …focus on personal information that is 'passed along' from an individual or entity to a different entity. It could ensure the pass along entity has the authority to do so and provides the receiving entity with the purpose for which the personal information may be used or disclosed. This would ensure that an entity receiving information being "passed along" has been given proper assurances by the first entity that the individual consented to that information transfer and the purposes for which that information may be used.[20]

7.18 The department responded to concerns about compliance and stated that to address compliance concerns, APP 4 includes a 'reasonable period' element within which to determine whether or not the entity could have collected the information under APP 3 if the entity had solicited the information, and a 'soon as practicable' test (rather than a requirement to do it immediately) relating to destruction or de-identification.[21]

7.19 The department also responded specifically to the concerns raised by Abacus and Westpac. It noted that under the process to determine whether the information could have been collected under APP 3, the entity would be able to determine which information was unsolicited (for example, a recorded phone call may involve standard questions being asked). The department went on to comment that the solicited information obtained in these instances would, in practice, be converted into other

---

17 Westpac, *Submission 13*, p. 2.

18 Abacus Australian Mutuals, *Submission 7*, p. 2.

19 Yahoo!7, *Submission 20*, p. 2.

20 Telstra, *Submission 19*, p. 2.

21 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 13.

means such as another form, a document or on a computer. Therefore, if the entity decided to destroy the electronic recording of the phone discussion, it would still have the solicited information.[22]

7.20 The department also noted that, as pointed out by Westpac, if it is not reasonable to do so, the entity is not required to destroy or de-identify the information (APP 4(4)).

7.21 In concluding its response to this concern, the department noted that the ALRC recognised that there was a need to clarify the meaning of 'unsolicited' personal information. In accepting this recommendation, the Government stated that it encouraged the development and publication of appropriate guidance by the OPC, noting that the decision to provide guidance is a matter for the OPC. While it is ultimately a matter for the Australian Information Commissioner, the department anticipates that the guidelines will address matters such as those raised by the Abacus Australian Mutuals and Westpac.[23]

Determining if information could have been collected under APP 3

7.22 Under APP 4(1), if an entity received unsolicited personal information it is required, within a reasonable period, to determine if it could have collected the information under APP 3 if it had solicited the information. The committee received a range of comments in relation to this provision.

7.23 The Health Services Commissioner, Victoria, commented that APP 4 may be difficult to implement in health settings and gave the example of a relative or other person providing unsolicited information about a client. The Commissioner noted that it would not be easy to determine if the information could have been collected under APP 3. The Commissioner recommended that consideration be given to how APP 4 would apply in the health care area and pointed to Victorian Health Privacy Principle 1.7(d) which deals with information provided in confidence.[24]

7.24 The ABA also commented on the need to ensure that the 'reasonable period requirement' allows entities sufficient time to meet the requirements of APP 4(1). Organisations such as banks have large volumes of information being provided by a wide range of sources. The ABA argued that what is determined to be 'within a reasonable period', must take account of the dimensions of this obligation to make the requisite determination. The ABA suggested that clarification of the term be provided by either a legislative note or by guidance from the OPC.[25]

---

22 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, pp 13–14.

23 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 14.

24 Health Services Commissioner, Victoria, *Submission 26*, p. 2.

25 Australian Bankers' Association, *Submission 15*, p. 5.

7.25 The Insurance Council of Australia also noted that large amounts of personal information, often unsolicited, are received by insurers and this would require time to evaluate under the proposed 'lawful and reasonable test'.[26]

7.26 The Law Council of Australia (LCA) raised the concern that APPs 4 to 6 do not 'expressly permit the sale of a medical business as a going concern'. The LCA noted that the relevant legislation in Victoria and the Australian Capital Territory provide useful examples of how this might be addressed.[27]

Destruction/de-identification of unsolicited personal information – APP 4(4)

7.27 APP 4(4) provides that where an entity determines that it could not have collected the unsolicited information under APP 3, it must, as soon as practicable and if lawful and reasonable to do so, either destroy the information or ensure that the information is no longer personal information. Comments received in relation to this provision of APP 4 went to the need for greater clarity of meaning of the terms used, the application of the provision in certain cases and the destruction requirement.

7.28 The Office of the Guardian for Children and Young People commented that the benefit of ensuring that the information is no longer personal information is unclear and creates confusion about what constitutes 'personal information'.[28] Abacus Australian Mutuals suggested that the words '(for example, by taking steps to remove any reference to the individual to whom the information relates)' should be added to the words 'no longer personal information' to provide greater clarity.[29]

7.29 The ABA recommended clarification of the term 'could not have collected' in APP 4(4) so that it means the collection is prohibited by law rather than simply because it is information that the individual could not provide. For example, the opinion given by a third party or information that is obtained in connection with an insurance claim where the insurer's duty of disclosure is in issue.[30]

7.30 The OIC and Privacy Law Consulting raised concerns about the effect of APP 4(4) in instances where personal information is provided in error to an agency and which, as a standard practice, the receiving agency forwards to the correct agency. It was argued by Privacy Law Consulting that APP 4 may prohibit this practice on the basis that, as soon as an agency receives any unsolicited personal information in this way, it is in effect generally obliged to destroy the information. The Office of the Information Commissioner, Queensland, suggested that to ensure that in such cases

26 Google, *Submission 17*, p. 2.

27 Law Council of Australia Privacy Committee, *Submission 31*, p. 2.

28 Office of the Guardian for Children and Young People, *Submission 4*, p. 4.

29 Abacus Australian Mutuals, *Submission 7*, p. 2.

30 Australian Bankers' Association, *Submission 15*, p. 5.

information could be passed on to the relevant agency, a form of wording such as the following could be added:

> If the entity determines that the entity could not have collected the personal information but is able to determine that another entity could have collected the personal information, the first entity can, as soon as practicable and only if it is lawful and reasonable to do so:
>
> (a) pass the information onto the appropriate entity; and
>
> (b) inform the individual about the passage.[31]

7.31 The department responded to these concerns and stated that correspondence received by Ministers, members of parliament and government departments and agencies would, in normal circumstances, be unsolicited. It is clear that the unsolicited information could have been collected under APP 3 because considering and responding to concerns of members of the public, and referring them to appropriate recipients, are functions of these entities. Once an entity has determined that the personal information could have been collected under APP 3, it would be possible for the entity to use or disclose the information under APP 6. Under that APP, disclosure to another Minister or government department would be permitted where the individual has consented to the use and disclosure. As the individual has written with queries, views or representations on particular issues, it is within their legitimate expectation that their correspondence will be referred to the appropriate entity within parliament or government.

7.32 The department went on to state that the recipient entity would also be receiving unsolicited personal information. However, it is also clear that it could have been collected under APP 3 because considering and responding to concerns of members of the public on the particular issues within its responsibilities are directly related to the functions or activities of the entity. The entity may then use the information for the purpose of responding to the correspondence.

7.33 The department concluded that therefore, the practice of agencies forwarding incorrectly addressed correspondence will not be prohibited under the new APPs.[32]

7.34 In relation to the destruction provision, the NSW Department of Justice and Attorney General pointed out that the ALRC recommendation would have allowed an agency, if it did not wish to retain unsolicited information, to destroy it without having to decide whether it could have collected the information under APP 3. In addition, the recommendation would have allowed the agency to destroy the information if it decided that it could have lawfully collected it, without the need to then comply with other privacy principles. The NSW Department of Justice and Attorney General

---

31 Office of the Information Commissioner, Queensland, *Submission 18*, p. 4.

32 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 14.

commented that 'it may be preferable to give agencies the option of destroying unsolicited information as the ALRC proposed'.[33]

7.35 The ABA submitted that a proportionate and workable approach to the application of this principle would be to require that the obligation to destroy or de-identify personal information applies only to solicited information received from third parties.[34] Privacy NSW suggested that sometimes it is appropriate to return unsolicited personal information to the sender rather than destroying it.[35]

7.36 The OIC also recommended including an example after APP 4(4) which demonstrates when it would be unlawful to destroy the personal information, and which includes a reference to the recordkeeping obligations of agencies.

7.37 Privacy Law Consulting raised two matters. First, it is not clear if the entity is permitted to use or disclose the information for any purpose prior to destroying or de-identifying it. Secondly, while the intention appears to be that unsolicited information contained in a 'Commonwealth record' can be destroyed under APP 4(4) provided destruction is in accordance with the Archives Act, the interrelationship of APP 4 with section 24 of the Archives Act 1983 should be clarified.[36]

Clarifying the relationship between collection and receiving

7.38 The OPC also suggested that a note or explanatory guidance should be provided to clarify that, in the context of APP 4(4), a technical 'collection' will not be a breach of APP 3 (such as unnecessary collection), if the 'collected' information was:

- unsolicited, but then
- dealt with appropriately in line with APP 4.[37]

Conclusion

7.39 The committee has considered submitters' comments in relation to the structure of APP 4. While it would appear that it may be beneficial to include the collection of unsolicited information in the 'collection' principle, APP 3, the committee is persuaded by the department's argument that a separate principle clarifies the Government's policy intent that unsolicited information should be provided with the same privacy protections as solicited information.

7.40 In relation to the compliance burden imposed by APP 4, the committee considers that there may be instances where entities experience an increased

---

33 NSW Department of Justice and Attorney General, *Submission 42*, p. 5.

34 Australian Bankers' Association, *Submission 15*, p. 5.

35 Privacy NSW, *Submission 29*, p. 4.

36 Privacy Law Consulting, *Submission 24*, p. 3.

37 Office of the Privacy Commissioner, *Submission 39*, p. 30.

compliance burden. However, the committee is mindful of the advice provided by the department that the 'reasonable period' aspect of the principle (in relation to determining if the information could have been collected under APP 3) and the 'soon as practicable' requirement (for destruction or de-identification) will address compliance concerns. The committee also believes that these elements will provide sufficient flexibility to allow entities to meet the obligations under this principle.

7.41 The committee notes the NSW Department of Justice and Attorney General's comments in relation to the ALRC's recommendation that would allow an agency, if it did not wish to retain unsolicited information, to destroy it without having to decide whether it could have been collected under APP 3. In addition, the recommendation would have allowed the agency to destroy the information if it decided that it could have lawfully collected it, without the need to then comply with other privacy principles. The committee considers such a provision may address compliance burden concerns; however, Commonwealth agencies, for example, must comply with the requirements of the *Archives Act 1983* in relation to the destruction of records. The committee considers that there may be merits for including such a provision but the interaction with other legislation would need to be considered.

7.42 The committee notes with regard to the interrelationship of APP 4 with the Archives Act, that the Government response to the ALRC's recommendations stated that guidance from the OPC 'would also clarify that the proposed principle does not affect the operation of the *Archives Act 1983* in relation to agencies'.[38]

7.43 There were a number of concerns raised in submissions about the term 'no longer personal information' and the committee considers that this term requires further clarification to ensure the aims of the principle are achieved.

Recommendation 9

7.44 The committee recommends that the term 'no longer personal information' contained in APP 4(4)(b) be clarified.

38 Australian Government, *Enhancing National Privacy Protection*, p. 41.

Chapter 8

Australian Privacy Principle 5–notification of the collection of personal information

Introduction

8.1 Australian Privacy Principle 5 (APP 5) stipulates that entities are obliged to notify an individual of certain matters at the time that the individual's personal information is being collected. In particular, an entity is required to ensure that the individual is aware of how and why the information will be collected and how the entity will manage the personal information.[1]

Background

8.2 The *Privacy Act 1988* does not contain an express obligation regarding notification. Rather, the relevant privacy principles which relate to the collection of personal information, provide that agencies and organisations are required, in particular circumstances, 'to ensure that an individual whose personal information has been, or is to be, collected, is aware of a number of specific matters'. Provisions along these lines are contained in both the Information Privacy Principles (IPPs) in relation to entities and the National Privacy Principles (NPPs) in relation to organisations.[2]

8.3 Where information is collected directly from the individual, IPP 2 and NPP 1.3 both list the matters which an individual should be made aware of before, or as soon as practicable after, their personal information is collected, or in the case of organisations under NPP 1.3, at the time of collection. NPP 1.5 also provides that in cases where information about an individual is collected from a third party, the individual must be made aware of the matters listed in NPP 1.3, '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'.

8.4 The ALRC's consideration of notification included:

- whether requirements relating to notification should be set out in a separate principle;
- the nature and timing of the obligation to notify;
- the circumstances in which an obligation to notify might arise; and

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 759.

- which matters an individual should be notified of when personal information is collected.[3]

8.5 The ALRC noted that there were examples in other jurisdictions of both a separate notification principle and notification requirements within the privacy principle regarding collection. The ALRC came to the view that requirements relating to notification of individuals should be provided in a discrete principle, as it plays an important role in the information cycle, promotes transparency and 'is essential in informing individuals about the treatment of their personal information, and their rights in this regard'.[4]

Obligation to notify

8.6 In respect of the obligation to notify, the ALRC noted that 'notification is one way of ensuring awareness.' The ALRC commented that while agencies and organisations should be required to notify or ensure that an individual is aware of specific matters regarding the handling of their personal information, it would be prescriptive to insist on notification in all cases. Indeed, insisting on notification could increase the compliance cost and burden for agencies and organisations, as well as possibly overloading individuals with information. Consequently, the ALRC formed the view that agencies and organisations could ensure that an individual is aware of required matters by drawing the individual's attention to specific parts of the privacy policy or other relevant documents. The ALRC suggested that guidance on the circumstances under which this would be acceptable should be issued by the Office of the Privacy Commissioner (OPC).[5]

8.7 The ALRC noted that ideally, obligations to notify should be complied with before, or at the time of collection of personal information, allowing the individual adequate opportunity to make an informed choice about disclosing their personal information. However, the ALRC recognised that it would be unreasonable to insist on compliance with this obligation in all circumstances and stated that the principle needs to be flexible enough to adapt to these circumstances. However, the ALRC noted that the agency or organisation 'will need to demonstrate the basis upon which impracticability is asserted, if the issue arises'.[6]

8.8 Agencies and organisations currently need to ensure individuals are aware of certain matters when information is collected directly from the individual; in addition

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 759–60.

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 760–63.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 766–67.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 767.

organisations are required to notify individuals if the information is collected from a third party. The ALRC considered that all agencies and organisations should be required to notify individuals of particular matters pertaining to the collection of their personal information, regardless of whether the information is collected directly from the individual or from a third party.[7]

Reasonable steps

8.9 Under the current provisions, organisations must take 'reasonable steps', and agencies are required to 'take such steps (if any) as are, in the circumstances, reasonable' to ensure that an individual from whom personal information is being collected, is aware of certain matters.[8] The ALRC considered both terms and formed the view that there may be circumstances in which it is reasonable for an agency or organisation to take no steps to notify or otherwise ensure an individual is aware of particular matters. The ALRC considered that this should be expressly provided for in the legislation, and that the OPC should issue guidelines addressing the circumstances in which it would be reasonable not to take any steps to notify individuals about the collection of their personal information.[9]

8.10 The ALRC further noted that providing the qualification that an agency or organisation only needs to take such steps, if any, as are reasonable in the circumstances ensures that the principles remain sufficiently high-level, so that they can be widely applied without having to incorporate any specific exceptions into the legislation itself.[10]

Matters for notification

8.11 The ALRC considered a series of matters which agencies and organisations might notify an individual of. The NPPs and IPPs both list various matters about which individuals must be made aware. However, while some of the matters share common ground, they are not consistent.[11]

8.12 The ALRC noted that notification is particularly important in light of existing and developing technology, as an individual may not always be aware that their personal information has been collected. The ALRC clarified that this obligation

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 779–82.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 768–69.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 768–73.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 778.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 783–84.

should not be imposed on agencies and organisations in circumstances in which it is clear that the individual is aware that their information has been collected – particularly in circumstances in which the individual provided the information themselves. The ALRC further noted that this requirement would be subject to the 'reasonable steps' test.[12]

8.13 The ALRC formed the view that both agencies and organisations should be obliged to notify individuals who they are collecting information from, of the following details:

- the collecting entity's identity;
- functional contact details for the collecting entity;
- the purpose for which the information is collected;
- the individual's right of access to and correction of, the personal information that they provide; and
- the main consequences of not providing the requested personal information.[13]

8.14 In addition, the ALRC noted that NPP 1.3 currently only requires organisations to ensure an individual is aware of other organisations that it usually discloses such information to; however, the OPC guidelines indicate that this should be interpreted broadly. Given the current obligations and the OPC guidelines, the ALRC formed the view that:

> 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.[14]

8.15 The ALRC also stated that the level of specificity provided to comply with this requirement would depend on the circumstances and should be the subject of guidance from the OPC.[15]

8.16 While it is not currently required to inform individuals of available avenues of complaint, the ALRC noted that the OPC had called for such a provision in its 2005 review, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988.* However, the ALRC did not support such an approach as this information should already be provided in the privacy policy. Drawing the individual's

---

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 784–87.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 787–89.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 794.

15 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 794.

attention to the fact that such avenues exist, and are set out in the privacy policy, should suffice.[16]

8.17 The ALRC considered that the obligations currently in place under the NPPs and IPPs regarding notification that collection of information is authorised or required under law, are similar but differ, as do the guidelines issued on each by the OPC. It was noted that IPP 2 appears less onerous than the obligation under the NPPs as it only requires an individual to be made aware of 'the fact' that the collection of information is authorised or required by or under law. However, the guidance provided on IPP 2 by the OPC takes a stricter approach, requiring an 'IPP 2 notice' to contain reference to the particular provisions of legislation which require or authorise the collection of information, whereas the guidance provided on the NPPs is more lenient.[17]

8.18 Noting that such an obligation is particularly important with regard to the agencies which have coercive information-gathering powers, the ALRC suggested that the current IPP obligation provided the most appropriate form of words for this requirement, and should be extended to apply to organisations as well. Consequently, the ALRC concluded that agencies and organisations '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.' This of course was to be complemented by guidance developed by the OPC.[18]

8.19 The ALRC also recommended that to facilitate compliance, the OPC should develop and publish guidance on matters including when it would be reasonable to take no steps and appropriate level of specificity when notifying individuals about anticipated disclosures.

Government response

8.20 In its response, the Government agreed that requirements relating to notification should be set out in a separate privacy principle. The Government further agreed that provision should be made in the principle for circumstances in which it would be reasonable for an entity not to take any steps to notify an individual about certain matters pertaining to the collection of their personal information, and that the OPC would be encouraged to provide guidance on such circumstances.[19]

---

16 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 794–96.

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 797–98.

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 797–98.

19 Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, pp 45–47.

8.21 The Government response indicated that it would make amendments to the ALRC's recommendation on the matters to be notified. It was noted that information on the fact and circumstances of the collection of an individual's personal information would only need to be provided in circumstances in which an individual was not aware that their personal information had been collected. Consequently, the Government suggested that the intent of this requirement might be better expressed in a different form.[20]

8.22 In addition, the Government indicated that agencies and organisations should identify the particular law under which the collection of the personal information is authorised, rather than simply the fact that the information is required by law. However, the response explained that it was expected that the particular provision under which the collection of information is required or authorised would not need to be identified.[21]

8.23 Community concern regarding the flow of personal information overseas was noted, and, in light of this, the Government stated that agencies and organisations should also be required to notify individuals whether their personal information is likely to be transferred overseas, and where it might be transferred to. However, the response recognised that an agency or organisation may not know at the time of collection whether the information would be transferred overseas, or the particular jurisdiction to which the information might be transferred, therefore, this requirement would be subject to the 'reasonable steps' test.[22]

Issues

8.24 The matters raised in relation to APP 5 went principally to the need for clarity, the interpretation of the reasonableness test and matters to be notified.

Structure and terminology

8.25 Submitters commented on the structure and complexity of the principle. APP 5 was supported by Privacy NSW, but it was suggested that the principle be simplified as follows:

> When an entity collects personal information it must notify the individual about the following matters, unless it is reasonably unable to do so [suggest that there be a reference to guidance by the Privacy Commissioner on these matters]:…[23]

8.26 The OPC also suggested that APP 5 be simplified and shortened, with APP 5(1) becoming a single provision, the removal of repeated phrases, and

---

20 Australian Government, *Enhancing National Privacy Protection*, p. 45.

21 Australian Government, *Enhancing National Privacy Protection*, p. 46.

22 Australian Government, *Enhancing National Privacy Protection*, p. 46.

23 Privacy NSW, *Submission 9*, p. 4.

incorporating APP 5(2) into APP 5(1). The OPC noted that this type of simplified structure would more closely reflect the structure of the existing NPP 1.3 and IPP 2.[24]

8.27 Professor Greenleaf and Mr Waters noted that there was some inconsistency in the terminology used in the exposure draft, as APPs 1, 5, and 8 use the term 'overseas', while elsewhere the phrase 'outside Australia' is used.[25] Professor Greenleaf and Mr Waters also commented that on the definition of term 'collects', as they argued that currently there is a risk that collection methods which do not involve a third party may be excluded from the requirements under APP 5. Consequently, Professor Greenleaf and Mr Waters suggested that:

> ...the definition of 'collects', should expressly include collection by observation, surveillance or internal generation in the course of transactions, to ensure that the notification principle is not read as applying only to collection resulting from 'requests'.[26]

8.28 In response to this matter, the Department of the Prime Minister and Cabinet (the department) commented that the ALRC found that it was unnecessary to amend the Privacy Act to refer to specific methods of collection because it was clear that personal information could be collected through lawful and fair means (as required by NPP 1) by surveillance, and from publicly available sources, such as books. In addition, the department stated the ALRC noted that OPC guidance on the requirement for 'fair and lawful' collection recognised 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. The department concluded:

> As the new draft does not alter the existing position that the means of collection of personal information must be 'lawful and fair' (see APP 3(4)), APP 3 or APP 5 do not expressly refer to 'observation, surveillance or internal generation'.

8.29 The Law Institute of Victoria (LIV) suggested that, in order to maintain consistency with earlier provisions in the legislation, the term 'collects' in APP 5(1) be replaced with 'receives', thereby also ensuring that both solicited and unsolicited information are covered by APP 5.[27]

8.30 The department commented on the LIV's suggestion and noted that the use of the term 'collects' is necessary in APP 5 to ensure consistency with the operation of, and terminology used in, APP 3 (collecting solicited information) and APP 4 (receiving unsolicited information). Pursuant to the provisions of APP 4, an entity upon receiving unsolicited personal information is to determine whether the entity

---

24 Office of the Privacy Commissioner, *Submission 39*, p. 31.

25 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10.

26 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 9.

27 Law Institute of Victoria, *Submission 36*, p. 6.

could have collected the information under APP 3 if the entity had solicited the information. If the answer to that is yes, APP 5 immediately applies as if the information had been 'collected' as solicited information and the notification requirements under APP 5 must be complied with. If the entity could not have collected the personal information, the entity must destroy or de-identify the information, as soon as practicable but only if it is lawful and reasonable to do so (APP 4(4)). There is no notification requirement in this instance because the personal information is not being retained for any purpose relating to the identification of the individual.[28]

8.31 The Law Council of Australia (LCA) expressed concern that as currently drafted the requirements relating to collection in APPs 4, 5 and 6 'do not, expressly permit the sale of a medical business as a going concern.' The LCA suggested that the legislation should:

> ...specifically allow the collection of sensitive information in circumstances where an entity is buying a medical business as a going concern. Principle 10 in the *Health Records Act 2001* (Vic) and Principle 11 of the *Health Records (Privacy and Access) Act 1997* (ACT) provide useful examples of how this issue might be addressed.[29]

Conclusion

8.32 In chapter 3, the committee made general comments on the structure of the APPs. The committee considers that further consideration should be given to the structure of APP 5 in light of those comments.

Possible impact of notification of collection

8.33 While Microsoft welcomed the flexibility introduced into APP 5(1) with the inclusion of the test of reasonableness, other submitters voiced concern about the lack of flexibility in relation to the consideration of the impact on individuals.[30]

8.34 Various submitters raised concerns about the possible implications of notifying individuals of the collection of information, noting that that this may result in the disclosure of information which may impact on the health, safety or privacy of other individuals. The Australian Bankers' Association (ABA) suggested that APP 5(2)(b) should make provisions to ensure that notification does not have an unreasonable impact on other individuals. The Office of the Guardian for Children and Young People (GCYP) requested guidance on the term 'reasonable in the circumstances', arguing that notifying individuals of the collection or disclosure of information may pose a risk to health and safety in some circumstances.

---

28 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 15.

29 Law Council of Australia, *Submission 31*, p. 5.

30 Microsoft, *Submission 14*, p. 10.

Consequently, the GCYP noted 'a risk assessment is required to determine if notification or the seeking of consent is safe, reasonable and appropriate'.[31]

8.35 In its submission, the GCYP suggested a series of considerations to be taken into account before seeking consent or notifying individuals of the collection or disclosure of personal information, designed to ascertain whether notification of, or seeking of consent for, the collection or disclosure of information is likely to cause harm to the individual, the public, or others.[32]

8.36 Abacus Australian Mutuals raised similar concerns, and noted that APP 5 does not contain the exceptions provided under NPP 1.5, which provides that individuals must be notified of collection of personal information, except where notification would pose a serious risk to the life or health of an individual. Abacus Australian Mutuals explained that its members have used these exemptions in the past, and argued that the exemptions should continue under future legislation.[33]

8.37 Abacus Australian Mutuals also expressed concerns that APP 5 could be inconsistent with the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act) tipping off obligations. Abacus Australian Mutuals explained that 'section 123 of the AML/CTF Act requires that an institution must not disclose to any non-AUSTRAC person that a suspect matter report (SUSMR) has been lodged (or that a suspicion has been formed that a SUSMR needs to be lodged).' To ensure clarity, it recommended that APP 5 be amended to explicitly state that any requirements to notify individuals of collection of personal information will be overridden if a tipping off issue exists.[34]

8.38 The Office of the Information Commissioner, Queensland (OIC), noted that the obligation to notify individuals of information provided by a third party under APP 5 raises practical issues. In terms of privacy, the OIC argued that it is not always practical or desirable to disclose information received by a third party; for example, in a confidential complaints process, the person being complained about would have to be notified, thereby compromising the confidentiality of the process. In addition, information is often quite routinely and legitimately passed between entities in the performance of their functions; for example, the Queensland Police Service will access the data held by the Queensland Department of Transport when dealing with traffic infringements. The OIC explained that in order to avoid these practical difficulties, Queensland's privacy legislation only obliges an entity to notify

---

31 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 6–7; Office of the Guardian for Children and Young People, *Submission 4*, p. 5; Australian Bankers' Association, *Submission 15*, pp 5–6.

32 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 6–7; Office of the Guardian for Children and Young People, *Submission 4*, p. 5; Australian Bankers' Association, *Submission 15*, pp 5–6.

33 Abacus Australian Mutuals, *Submission 7*, p. 2.

34 Abacus Australian Mutuals, *Submission 7*, p. 2.

individuals of collection of information if the information is collected directly from the individual.[35]

8.39 Despite its concerns, the GCYP agreed that seeking informed consent for the collection or disclosure of personal information, and providing advice about the purpose of the collection of personal information, and to whom the information may be disclosed, at the time of the collection, is preferred and recommended where it is safe to do so.[36]

Conclusion

8.40 The committee notes that the ALRC review concluded that there are certain circumstances in which it would be reasonable for an agency or organisation not to notify an individual of particular matters pertaining to the collection of their personal information. The Government response agreed with this conclusion. Consequently, the exposure draft of APP 5 provides that any obligation to notify is subject to the 'reasonable steps' test, which provides that 'the entity must take such steps (if any) as are reasonable in the circumstances'.[37] This recognises that there may be circumstances in which it would not be reasonable to take any steps to notify an individual of particular matters regarding the collection of their personal information.[38]

8.41 The Government further supported the ALRC's recommendation that the OPC should issue guidelines on the circumstances in which it would be reasonable to not take any steps to notify an individual. In its report, the ALRC provided a list of circumstances which the guidance should address, as circumstances in which it may be reasonable to take no steps to notify.[39] The committee notes that the list includes provision for circumstances in which:

- notification would pose a serious threat to the life or health of an individual;
- notification would prejudice the enforcement of laws, or the prevention, detection, investigation and prosecution of offences, breaches of a law imposing penalty or seriously improper conduct; and

35 Office of the Information Commissioner, Queensland, *Submission 18*, pp 3–4.

36 Office of the Guardian for Children and Young People, *Submission 4*, p. 5.

37 *Australian Privacy Principles Exposure Draft*, ss 6(1).

38 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 772–73; Australian Government, *Enhancing National Privacy Protection*, p. 45.

39 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 772–73; Australian Government, *Enhancing National Privacy Protection*, p. 45.

- non-compliance with the principle is required or authorised under law.[40]

8.42 The committee therefore considers that the 'such steps (if any) as are reasonable in the circumstances' provisions of APP 5, in conjunction with guidance from the Australian Information Commissioner, provides appropriate flexibility to the notification principle to address concerns raised by submitters.

Compliance and notification via privacy policy

8.43 A number of submitters noted strong support for the provision for the notification of collection or disclosure of personal information, as an enhancement of the current requirements.[41] The Office of the Victorian Privacy Commissioner (Privacy Victoria) noted that the provision of information through a notice to an individual ensures that 'individuals are aware of their rights and obligations in respect to giving up (and later accessing) their information', and differs from the provision of information through a privacy policy which is not as comprehensive and often provides more general information.[42]

8.44 However, other submitters sought clarification of how they might ensure they comply with APP 5. Submitters also discussed whether notification obligations could be sufficiently discharged by referring individuals to a privacy policy.

8.45 A series of submitters noted that the notification requirements under APP 5 would create an additional compliance burden for entities, particularly as entities often receive large amounts of unsolicited information.[43] The Australian Institute of Credit Management suggested that this principle should be phased in to ameliorate the possible compliance burden and associated costs.[44]

8.46 The Australian Hotels Association requested guidance as to whether providing signage containing the required privacy information stipulated under APP 5 at the entry of a venue using ID scanning technology would provide sufficient compliance with the Act.[45]

8.47 Telstra Corporation Limited (Telstra) queried whether APP 5 would require an entity to provide a notification every time a collection activity is undertaken. As

---

40 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 772–73.

41 See Office of the Victorian Privacy Commissioner, *Submission 5*, pp 6–7; Australian Institute of Credit Management, *Submission 8*, p. 3; Yahoo!7, *Submission 20*, pp 1–2.

42 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 6–7.

43 See Australian Institute of Credit Management, *Submission 8*, p. 3; Office of the Information Commissioner, Queensland, *Submission 18*, p. 3; National Australia Bank, *Submission 2*, pp 3–4.

44 Australian Institute of Credit Management, *Submission 8*, p. 3.

45 Australian Hotels Association, *Submission 22*, p. 3.

Telstra confirms customer details at every transaction, if new details are provided, APP 5 could require Telstra to provide a notification at each transaction, which would be administratively burdensome, and could result in the customer being overwhelmed with notices. Telstra argued that it would be more effective to provide customers with a comprehensive privacy policy at the start of their relationship with the entity, to avoid multiple notices. Telstra submitted that APP 5 should be amended to clearly indicate that an entity can adequately discharge its obligations regarding notification by taking reasonable steps to bring its privacy policy to an individual's attention.[46]

8.48 A similar concern was raised by the Financial Services Council (FSC), which requested clarification as to what constitutes 'reasonable steps' to enable the entity to determine whether continuous disclosure notifications are necessary for existing relationships once the initial disclosure is made at the first meeting. FSC also suggested that these requirements might sufficiently be met by referring an individual to information on the entity's website.[47]

8.49 Microsoft expressed concern that increasing requirements for entities to provide notices to individuals does not necessarily provide a real benefit to individuals, who:

> ...can be overwhelmed but not enlightened by long privacy policies or disclosure statements, even where intended to allow informed consent. This emphasis does not take into account the realities of the way high volumes of personal information are collected used and disclosed in the current and rapidly evolving IT environment let alone the continued aggregation and sharing by third parties. It leaves individual users bearing the risk in circumstances where they are not equipped, and as research is showing, not willing, to bear it.[48]

8.50 Microsoft suggested an alternative approach in providing 'layered' privacy notices, which present short bullet-point summaries of an entity's practices, with links to the full privacy statement for those who require more detailed information. Microsoft suggested this would reduce the compliance obligations on entities, and the information load on individuals, while still making more detailed information available for those who are interested.[49]

8.51 However, Privacy NSW suggested that notification of the matters under APP 5 provided an opportunity to allow individuals to exercise express consent for the intended use and disclosure of their personal information via an 'opt-in' box.[50]

---

46 Telstra Corporation Limited, *Submission 19*, pp 2–3. See also Australian Hotels Association, *Submission 22*, p. 3.

47 Financial Services Council Ltd, *Submission 34*, p. 2.

48 Microsoft, *Submission 14*, p. 10.

49 Microsoft, *Submission 14*, pp 10–11.

50 Privacy NSW, *Submission 29*, p. 4.

Conclusion

8.52 The committee notes that the ALRC recognised the issues of compliance burden and cost for entities, and information overload of individuals. The ALRC explained that in order to reduce compliance costs and burden, and avoid unnecessary duplication, in some 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.[51]

8.53 The ALRC recommended that the OPC issue guidance on the circumstances in which it would be appropriate for an agency or organisation to refer an individual to particular sections of its privacy policy or other documents to comply with notification obligations. The Government also encouraged the development of appropriate guidance by the OPC, but noted that the decision to provide guidance is a matter for the Privacy Commissioner.[52]

8.54 The committee further notes that in the ALRC's list of circumstances in which it may be reasonable to not take any steps to notify an individual, the ALRC includes circumstances in which an entity collects personal information from an individual 'on repeated occasions'.[53]

Notification of matters –APP 5(2)

8.55 APP 5(2) provides for the matters that an individual is to be made aware of when personal information is collected.

Identity and contact details–APP 5(2)(a)

8.56 Professor Greenleaf and Mr Waters suggested that in order to prevent entities from providing individuals with contact details which are no longer current, this paragraph should specifically require the provision of the '*functional* contact details' of the entity.[54]

---

51 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 766–67.

52 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 804; Australian Government, *Enhancing National Privacy Protection*, p. 47.

53 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 773.

54 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 9.

Collection from third parties or if individual unaware–APP 5(2)(b)

8.57 APP 5(2)(b) provides that an individual must be notified that the entity collected, or so collects personal information from a third party or if the individual is unaware that the entity has collected the personal information. The National Australia Bank (NAB) expressed concern that as currently drafted, APP 5(2)(b) constitutes an absolute obligation. NAB noted that in some circumstances it may 'be unlawful, or interfere with the lawful functions of an entity (particularly enforcement bodies)' to inform individuals that an entity has collected their personal information, and consequently, such notification should only be required when it is 'reasonable and practical to do so'.[55]

8.58 The Australian Finance Conference (AFC) suggested that the two alternatives suggested under APP 5(2)(b) should be 'cumulative rather than alternative', and recommended that the word 'or' at the end of subparagraph (i) should be changed to 'and'. In effect this would only require an entity to notify the individual when information is collected from a third party without the individual's knowledge.[56]

Required or authorised by or under Australian law–APP 5(2)(c)

8.59 A series of submitters argued that the requirement to provide the name of the law or order of a court or tribunal which authorises or requires the collection of the personal information is onerous, and would be costly to comply with. Submitters noted that compliance with this requirement by the financial services sector would be particularly impractical, as the sector is regulated by a number of laws which either directly or indirectly require financial institutions to collect personal information from customers. In order to ensure that all relevant laws and court orders are appropriately identified, entities operating in similarly complex regulatory environments may need to obtain legal advice, incurring further costs.[57] The ABA suggested that it should be sufficient to provide a generic statement about the laws which authorise or require the collection of personal information, rather than identifying each individual law.[58]

8.60 The AFC also expressed concern that regulation requiring detailed disclosure from industry appears to be at odds with the Government's moves to encourage industry to adopt a 'simple but comprehensive approach' to reduce the volume of documentation which is provided to individuals to comply with disclosure obligations.[59] The AFC noted that APP 5(2)(c) would be tempered by the test of reasonableness included in APP 5(1), and consequently it may not be deemed

---

55 National Australia Bank, *Submission 2*, p. 3. See also paragraphs 8.33–8.42 regarding the possible impact of notification of collection.

56 Australian Finance Conference, *Submission 12*, p. 5.

57 National Australia Bank, *Submission 2*, pp 3–4; Australian Bankers' Association, *Submission 15*, pp 5–6; Australian Finance Conference, *Submission 12*, pp 5–6.

58 Australian Bankers' Association, *Submission 15*, p. 6.

59 Australian Finance Conference, *Submission 12*, pp 5–6.

reasonable in the circumstances to name the particular law or order which requires or authorises collection. However, to ensure clarity the AFC recommended the removal of the prescriptive requirement to name the relevant law or order from APP 5(2)(c).[60]

8.61 The NAB put another view and argued that as APP 3 protects individuals from the 'unnecessary' collection of personal information, APP 5(2)(c) is unlikely to provide a real benefit to individuals.[61] Further, NAB noted that the requirement under APP 5(2)(c) was not included in the ALRC's recommendations, and suggested that the legislation should reflect the ALRC's original recommendation, ensuring that individuals be notified of the 'fact, where applicable, that the collection is required or authorised by or under law'.[62]

8.62 However, Professor Greenleaf and Mr Waters presented a different view noting their support for the requirement to specify the relevant Australian law or court or tribunal order in the notice to an individual. They explained that this would ensure that individuals receive the adequate level of detail in notifications, as currently entities can get away with providing unhelpful and generalised information to individuals.[63]

Consequences to the individual–APP 5(2)(e)

8.63 The LIV commented that while this provision requires an entity to advise an individual of the consequences of not providing information, it is not evident that there is any regulation of whether the said consequences of not providing information are fair and reasonable. Further, there is no provision requiring the entity to inform the individual of their right not to provide identity information. The LIV recommends that such a provision be incorporated into APP 5(2).[64]

Disclosure to third parties–APP 5(2)(f)

8.64 Professor Greenleaf and Mr Waters noted some inconsistency in terminology in this paragraph, with the introduction of the term 'body'. They suggested that the other two terms used in the paragraph, 'entity' and 'person', are employed elsewhere in the legislation and would appear to adequately convey the meaning required.[65]

8.65 In comparing this provision with the NPPs and IPPs, the OPC raised concern about the lack of specificity in this provision, noting that as currently drafted, it could be interpreted as requiring that notice be provided about information that the entity

60 Australian Finance Conference, *Submission 12*, pp 5–6.

61 National Australia Bank, *Submission 2*, pp 3–4.

62 National Australia Bank, *Submission 2*, pp 3–4.

63 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 9.

64 Law Institute of Victoria, *Submission 36*, p. 6.

65 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 9.

collects '*more generally*'. Notice which relates to the general sort of information collected by an entity would be lengthier and not as relevant or useful to an individual, and could probably be covered by a general privacy policy, rather than a specific notification. Consequently, the OPC suggested that this provision should specifically refer to the kind of information actually collected, in a similar manner to the NPPs and IPPs.[66]

Entity's privacy policy–APP 5(2)(g) and APP 5(2)(h)

8.66 The Health Services Commissioner, Victoria, noted its support for the requirement to notify an individual of the complaint mechanisms an entity has in place. However, Professor Greenleaf and Mr Waters expressed concern that these paragraphs provide 'indirect notice of actual mechanisms' by pointing individuals to the entity's privacy policy rather than providing them with direct information about the access, correction and complaint mechanisms in place. They suggested that in both APP 5(2)(g) and APP 5(2)(h), all words prior to 'how the individual may' be omitted, to ensure individuals are provided with express and direct information about the mechanisms in place.[67]

Disclosure to overseas recipients–APP 5(2)(i) and APP5(2)(j)

8.67 Professor Greenleaf and Mr Waters, and the Health Services Commissioner, indicated their support for the inclusion of a specific obligation to provide individuals with details regarding the transfer of information to overseas recipients. However, some concern was expressed about the inclusion of the qualification 'if it is practicable'. Professor Greenleaf and Mr Waters argued that this qualification is subjective, and as a result, many companies may use this as justification for not providing the information required under APP 5(2)(j).[68]

8.68 Other submitters raised concerns with this as it was seen as onerous, administratively burdensome and costly to comply with.[69] Coles Supermarkets Australia Pty Ltd (Coles) explained that as it outsources a number of services to contractors, the possibility of personal details being disclosed overseas, and the location of the overseas recipients, can change according to the operations and infrastructure arrangements of the service provider engaged. The ABA further noted that if the entity does not control the location of the overseas recipient, if the overseas

66 Office of the Privacy Commissioner, *Submission 39*, pp 31–32.

67 Health Services Commissioner, Victoria, *Submission 26*, p. 2; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 9.

68 Health Services Commissioner, Victoria, *Submission 26*, p. 2; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10.

69 Coles Supermarkets Australia, *Submission 10*, p. 2; Deloitte Touche Tohmatsu, *Submission 28*, p. 1; National Australia Bank, *Submission 2*, p. 2; Australian Finance Conference, *Submission 12*, p. 6; and Australian Bankers' Association, *Submission 15*, p. 3.

recipient relocates without the entity's knowledge, the entity will be in breach of the APPs.[70]

8.69 In addition, Privacy Law Consulting Australia and Coles argued that this obligation could potentially force the disclosure of information about entities' resources and operational arrangements which may be considered commercial in confidence information.[71]

8.70 The ABA expressed some uncertainty as to whether the requirement to name the country in which any overseas recipient may be located in APP 5 has the same meaning as APP 1. The ABA noted concern that the requirement under APP 5 could be read as requiring more specific information about the disclosure of personal details which are to be, or have been collected, significantly increasing the compliance burden on entities.[72]

8.71 While generally supportive of APP 5, Yahoo!7 expressed some concerns about the practicality of these particular provisions given the evolution of technology and the advent of cloud computing:[73]

> We consider international data transfer and back up to be ubiquitous in the online services industry especially when you consider cloud computing phenomena. We are concerned that it may not be practical to require companies to specify which countries they transfer data to in their privacy policies and favour a simple disclosure obligation which refers to international data transfer and back up more generally.[74]

8.72 A series of submitters commented that it is not clear how the requirement to notify an individual of which countries an entity is likely to disclose personal information to, will deliver any real benefit to individuals, as it simply notifies individuals where the information is going, not how it will be managed, or what level of privacy protection exists in that jurisdiction. Privacy Law Consulting Australia supported this view, stating that the provisions do not:

> ...require an organisation to state the name of the recipient, the purpose for which the information is disclosed or the nature of the activities of, or goods or services provided by, the recipient. Accordingly, the provisions do

---

70 Coles Supermarkets Australia, *Submission 10*, p. 2; Deloitte Touche Tohmatsu, *Submission 28*, p. 1; Australian Bankers' Association, *Submission 15*, p. 7.

71 Coles Supermarkets Australia, *Submission 10*, p. 2; Privacy Law Consulting Australia, *Submission 24*, p. 1; National Australia Bank, *Submission 2*, p. 2; Australian Finance Conference, *Submission 12*, p. 6; Australian Bankers' Association, *Submission 15*, p. 7.

72 Australian Bankers' Association, *Submission 15*, p. 7.

73 'In simple terms, cloud computing is a way to enhance computing experiences by enabling users to access software applications and data that are stored at off-site datacenters rather than on the user's own device or PC or at an organisation's on-site datacenter'. See Microsoft, *Submission 14*, p. 5.

74 Yahoo!7, *Submission 20*, pp 1–2.

> not result in consumers being provided with a level of information that will enable them to properly consider privacy issues associated with the overseas disclosure.[75]

Further, both ABA and NAB noted that in their consideration APP 8 provides adequate protections in this respect.[76]

Conclusion

8.73 In relation to the matters to be notified (APP 5(2)), much of the evidence argued that there was a lack of flexibility available to entities in the matters to be notified. For example, the NAB commented that there is an 'absolute obligation', even when it may 'be unlawful, or interfere with the lawful functions of an entity (particularly enforcement bodies)', to inform individuals that an entity has collected their personal information. Other submitters pointed to the compliance burden imposed by the requirement to provide the name of the law which requires the collection of personal information and the list of countries where an overseas recipient is located.

8.74 The committee notes the ALRC's view that:

> 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.[77]

8.75 As noted previously, the ALRC listed various circumstances in which it may be reasonable for an agency or organisation to not take any steps to notify an individual of certain matters regarding the collection of personal information (see paragraph 8.41). The Government accepted the ALRC's recommendation and also noted that there may be circumstances where it may be reasonable to take no steps to notify an individual about the collection of personal information. In addition, the Government response specifically commented that the 'reasonable steps' test applies to the requirements to notify individuals if their information is likely to be transferred overseas and to where it might be transferred:

> ...an agency or organisation would not need to include this information in a collection notice if it did not reasonably know at the time of collection whether information will be transferred overseas.

---

75 Privacy Law Consulting Australia, *Submission 24*, p. 1.

76 National Australia Bank, *Submission 2*, p. 2; Deloitte Touche Tohmatsu, *Submission 28*, p. 1; Australian Finance Conference, *Submission 12*, p. 6; Australian Bankers' Association, *Submission 15*, pp 3 and 7; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10; Privacy Law Consulting Australia, *Submission 24*, p. 1; Coles Supermarkets Australia, *Submission 10*, p. 2.

77 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 782.

> Further, it would not be reasonable to provide specific information if the organisation or agency does not reasonably know to which specific jurisdiction personal information may be transferred.[78]

8.76 The exposure draft of the notification principle reflects the Government view that there should be a reasonableness test for each of the matters to be notified. This is provided for as all of APP 5(2) is subject to the 'reasonableness' test of APP 5(1) as the linkage is given by the term 'matters' in APP 5(2) which links back to APP 5(1)(a). The additional test in APP 5(2)(j) is one of practicality concerning the notification of the range of recipient countries.

8.77 The committee concludes that the inclusion of the reasonableness test and that in some circumstances no steps need by taken, provides entities with the appropriate level of flexibility in relation to the notification of matters.

8.78 In relation to the need to notify an individual about the law under which information was collected, the ALRC report took the less stringent view that agencies and organisations should be required 'to notify, or otherwise ensure that an individual is aware of, the fact that the collection is required or authorised by or under law.' The ALRC also considered that the OPC should develop guidelines to assist agencies and organisations to comply with the provision.[79] However, the Government response indicated that the Government preferred that the principle clearly convey the expectation that the name of the relevant law be provided as a minimum. The Government response stated that:

> ...agencies or organisations should identify the specific law that requires or authorises the collection of information, though it would not be necessary to identify a specific provision.[80]

8.79 While this provision provides a higher level of specificity, the application of the reasonableness test will provide entities with flexibility.

8.80 In relation to the obligation to notify a person that certain matters are contained in the entity's privacy policy, the committee notes the ALRC's conclusion that agencies and organisations could fulfil their notification obligations by drawing an individual's attention to specific parts of the privacy policy or other relevant documents to ensure that an individual is aware of required matters. The committee also observes the ALRC's suggestion that the OPC should issue guidance on the circumstances under which this would be acceptable.[81]

---

78 Australian Government, *Enhancing National Privacy Protection*, p. 46.

79 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 798.

80 Australian Government, *Enhancing National Privacy Protection* , p. 46.

81 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 766–67.

8.81 Finally, the committee notes that the Government response supports the provision of guidance by the Australian Information Commissioner to assist entities in complying with the notification principle.

Chapter 9

Australian Privacy Principle 6–use or disclosure of personal information

Introduction

9.1 Australian Privacy Principle 6 (APP 6) outlines the circumstances in which entities may use or disclose personal information that has been collected or received.[1]

9.2 The Companion Guide states that from this principle, it is implicit that an entity may use or disclose personal information for the primary purpose that the information was collected for. This personal information can only be used or disclosed for a secondary purpose (a purpose other than the primary purpose), if the individual concerned has consented.[2] However, the Companion Guide explains that in some circumstances, the public interest outweighs individual privacy, and consequently a series of exceptions which allow the use or disclosure of personal information without consent, are provided for in APP 6. The exceptions are based on those which currently exist under National Privacy Principle 2.1, with the addition of some new exceptions. Further, this principle does not apply to the use or disclosure of government related identifiers or personal information for the purposes of direct marketing – use and disclosure for these purposes is covered in separate principles.[3]

Background

9.3 Provisions regarding the use and disclosure of personal information by agencies are contained in Information Privacy Principles (IPPs) 9 to 11. These provide that:

- personal information should only be used for a purpose which is relevant to the information (IPP 9);
- personal information should only be used for particular purposes for which it was collected unless certain exceptions apply (IPP 10);
- personal information should not be disclosed to a person, body or agency other than the individual unless certain exceptions apply (IPP 11).[4]

9.4 National Privacy Principle (NPP) 2 provides for the use and disclosure of personal information by organisations. Under NPP 2 the use and disclosure of

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

2 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

3 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

4 *Privacy Act 1988*, ss. 14(9)-ss. 14(11).

personal information for a purpose other than the 'primary purpose' of collection, is prohibited, unless certain exceptions apply.[5]

9.5 The NPPs and IPPs contain some similar exceptions, permitting the use and disclosure of personal information in situations in which:

- the individual consents to the use or disclosure;
- use or disclosure of the personal information is authorised by or under law;
- use or disclosure of the personal information is necessary to lessen or prevent a serious and imminent threat to the life or health of an individual;
- use or disclosure is reasonably necessary to enforce certain activities of an enforcement body.[6]

9.6 However, NPP 2 contains a much larger list of exceptions than the IPPs.[7]

9.7 In its review, the ALRC considered, amongst other issues:

- the appropriateness of consolidating the use and disclosure provisions in the IPPs and NPPs into a single principle;
- the circumstances in which the use and disclosure of personal information for a purpose other than the purpose the information was collected for, should be permitted; and
- whether any use or disclosure for a purpose other than the original purpose for which the information was collected, should be recorded.[8]

9.8 The ALRC considered whether use and disclosure provisions should be consolidated into a single principle and came to the view that a single privacy principle should deal with use and disclosure for both agencies and organisations. The ALRC commented that this would reduce the complexity of privacy regulation and avoid technical legal arguments about whether an action constitutes a use or disclosure.[9]

9.9 The ALRC noted that the principles in both the IPPs and NPPs relating to use and disclosure 'adopt a prescriptive approach' and do not contain an overriding qualifier such as permitting disclosure where it is 'reasonable' in the circumstances.

---

5 *Privacy Act 1988*, schedule 3, clause 2.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 839.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 839–40.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 838.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 840–44.

Use and disclosure of personal information is permitted for the primary purpose for which it was collected unless an exception authorises this action. The ALRC noted that these exceptions do not require the use or disclosure of personal information – they merely permit the use or disclosure in certain circumstances.[10]

9.10 The ALRC considered the exceptions to the prohibition on use or disclosure and came to the view that the exceptions as they apply to agencies and organisations should be consolidated. In addition, the ALRC commented, in relation to specific exceptions as follows:

- use or disclosure for a secondary purpose where there is a requisite connection with the primary purpose of collection, and within the reasonable expectations of the individual–the NPPs include this exception and the ALRC considered that it should also apply to agencies. In relation to sensitive information, the ALRC recommended that the secondary purpose be directly related to the primary purpose. The reasonable expectation test was seen as balancing the loosening of the provisions governing agencies and is unlikely to be particularly onerous;[11]
- authorisation of the use or disclosure of personal information in circumstances in which an individual has consented to that use or disclosure–this exception should be included in the use and disclosure principle;[12]
- use or disclosure of information in circumstances by agencies and organisations where they have reason to suspect unlawful activity–the ALRC considered this an appropriate exception but that it should only apply if such use or disclosure is a necessary part of the entity's investigation. The ALRC did not think it was necessary to expressly extend the exception to suspected serious misconduct, despite submissions to that effect by some stakeholders, as the OPC's guidance on investigation includes investigation of professional misconduct;[13] and
- law enforcement and regulatory purposes–the ALRC support an exception for the use or disclosure of information for a secondary purpose if it is necessary for, or on behalf of, an enforcement body to perform its functions. Rather than the more general exception in IPPs 10 and 11, the ALRC preferred the format

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 845.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 850–51.

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 852–53.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 862–63.

of NPP 2.1(h) in this regard as it listed specific functions to which such an exception would apply.[14]

9.11 In relation to the emergency, disaster and threat to life, health or safety exception, currently, personal information can be used and disclosed if it is necessary to lessen or prevent a serious and imminent threat to an individual's life or safety. The NPPs also allow secondary use and disclosure in certain circumstances. The ALRC formed the view that the use and disclosure of personal information should be permitted if an agency or organisation reasonably believes that such a use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, or the health and safety of an individual or the public. The ALRC explained the 'reasonable belief' test was an important safeguard, as an agency or organisation 'will need to have reasonable grounds for its belief that the proposed use or disclosure is essential, and not merely helpful, desirable, or convenient.'[15]

9.12 While an assessment of what constitutes a 'serious threat' would have to consider both the likelihood of harm, and the gravity of the outcome, the ALRC considered it prudent to retain this term. However, the ALRC suggested that the requirement that any threat be 'imminent' be removed, as it focuses on the immediacy of a threat, and in the ALRC's view, agencies and organisations 'should be able to take preventative action to stop a threat from escalating to the point of materialisation.'[16]

9.13 In its submission to the Legal and Constitutional Affairs Committee inquiry, the Australian Privacy Foundation suggested that the exception regarding the use or disclosure of personal information required or authorised by or under law should be restricted by removing the terms 'authorised' and under to remove any subjectivity, and providing a clear definition of what is encompassed by the term 'law'.[17]

9.14 The ALRC expressed the view that there must be provision for an exception which allows the use or disclosure of personal information where it is required or authorised by or under law. The ALRC noted suggestions that this exception should be narrowed, however the ALRC argued that restricting the exception might have 'far-reaching, and possibly unintended, consequences.' The ALRC suggested some important safeguards on this exception, recommending that the Privacy Act be amended to specify what is included by 'law' with regard to this exception, and suggesting that the OPC develop guidelines regarding when an act or practice will be

---

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 866–69.

15 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 859–60.

16 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 859–60.

17 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, Australian Privacy Foundation, *Submission 32*, p. 20.

required or authorised under law. Further, the ALRC explained that agencies and organisations must:

> ...be able to establish the basis upon which they assert their entitlement to rely on the exception. That is, they will still need to be able to identify the law which they assert requires or authorises a particular use or disclosure.[18]

9.15 While neither the IPPs nor the NPPs provide for the use and disclosure of personal information necessary for the purposes of confidential alternative dispute resolution (ADR) processes, the ALRC recommended that such an exception be included. The current Privacy Act, without such an exception, has the potential to present significant barriers to the resolution of disputes through ADR, which is 'facilitated by the disclosure of all relevant information by the parties to dispute resolution bodies, including personal information about third parties.'[19]

9.16 In providing this recommendation, the ALRC noted that ADR 'potentially could include an extremely broad range of situations.' The ALRC considered that the most appropriate way to limit the scope of the provision would be to provide confidentiality requirements, and the particulars of what constitutes confidentiality requirements would be articulated by guidance formulated by the OPC in consultation with the National Alternative Dispute Resolution Advisory Council.[20]

9.17 The ALRC considered the inclusion of an exception allowing use and disclosure for the establishment, pursuit or defence of legal rights. However, the ALRC came to the conclusion that such an exemption would not practically assist intending litigants in a substantial way, as the exception would permit and not compel the disclosure of information. Further, the ALRC noted that processes via court orders exist for the purposes of obtaining information for the purposes of legal rights, and that these processes are subject to established rules to prevent any abuse by the parties involved, and therefore provide the most appropriate way of accessing required information for these purposes.[21]

9.18 In its report, the ALRC noted the significant issues and competing considerations surrounding the authorisation for the use and disclosure of personal information for the purposes of missing persons investigations. While such disclosures may assist in locating missing persons who want to be located, it was noted that there are circumstances in which the missing person does not wish to be located for personal reasons, or due to fear for their own safety. In light of this, the ALRC noted

---

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 863–66.

19 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 870 and 1490.

20 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1491–92.

21 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1493–97.

that creating a general exception regarding missing person investigations could interfere with the privacy of an individual and risk their safety. The ALRC concluded that other means may be used to obtain information to assist missing persons investigations:

> Where an agency or organisation has a legitimate reason to search for a missing person, it may be able to avail itself of one of the other exceptions to the general prohibition in the 'Use and Disclosure' principle, or it may seek a public interest determination.[22]

Recording use or disclosure for a secondary purpose

9.19 The ALRC formed the view that, as is currently the case under IPPs 10 and 11 and NPP 2, agencies and organisations should be required to record any use or disclosure made under the exception regarding law enforcement. The ALRC noted calls from other committees and stakeholders for expanding the requirements regarding the logging of use and disclosures made for purposes other than the primary purpose of collection. However, the ALRC concluded that requiring that each use and disclosure made under an exception be recorded would not be justified and would be hugely impractical, costly and onerous for organisations and agencies.[23]

Government response

9.20 The Government accepted that a use and disclosure principle was necessary and that these requirements should 'be balanced so as to recognise other important public interests that may, on occasion, compete with the public interest of maintaining the individual's privacy'. The Government also agreed that the use and disclosure of personal information should be allowed for a secondary purpose if the individual would reasonably expect their information to be used for the secondary purpose, and the secondary purpose is related to the primary purpose of collection, or in the case of sensitive information, the secondary purpose is directly related to the primary purpose of collection.[24]

9.21 The Government response also indicated that, in addition to the exceptions recommended by the ALRC, it considered that further exceptions were necessary relating to circumstances in which:

- the individual consents to the use or disclosure;

---

22 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 874–75.

23 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 881–85.

24 Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, p. 52.

- unlawful activity or serious misconduct is suspected and the agency or organisation uses or discloses personal information as a necessary part of its own investigation of the matter or in reporting its concerns to relevant persons or authorities;
- the use or disclosure is required or authorised by or under law; and
- the organisation or agency reasonably believes that the use or disclosure is reasonably necessary for the prevention, investigation, detection or prosecution of breaches of a law by or on behalf of an enforcement body.[25]

9.22 The Government also identified additional exceptions related to matters addressed in other recommendations made by the ALRC in relation to confidential alternative dispute resolution; research purposes; and provision of a health service.

9.23 In agreeing that there should be provision for the use and disclosure of personal information where an agency or organisation reasonably believes it is necessary to lessen or prevent a serious threat to an individual's life, health or safety or public health or public safety, the Government acknowledged the concerns of some stakeholders that the exception was too broad. While the Government agreed with the removal of the term 'imminent', the response suggested that in order to provide an adequate safeguard, an additional requirement that it be unreasonable or impracticable to obtain an individual's consent to such a use or disclosure, be added to the exception.[26]

9.24 The Government indicated its support for an express exception to allow the use or disclosure of information for a missing person investigation. Recognising that there are legitimate reasons why some individuals may not wish to be located, the Government outlined that the exception would only permit, and not compel, the use or disclosure of personal information in these circumstances. Further, the Government stated that any use or disclosure of personal information for this purpose would be subject to binding rules issued by the Privacy Commissioner in a legislative instrument subject to parliamentary scrutiny. The Government suggested that the rules issued by the Privacy Commissioner should be developed in consultation with relevant stakeholders, and should address matters including that uses and disclosures should only be in response to requests from appropriate bodies with recognised authority for investigating reported missing persons; and where it is either unreasonable or impracticable to obtain consent from the individual, any use or disclosure should not go against any known wishes of the individual.[27]

25 Australian Government, *Enhancing National Privacy Protection*, p. 52.

26 Australian Government, *Enhancing National Privacy Protection*, pp 54–55.

27 Australian Government, *Enhancing National Privacy Protection*, pp 52–53.

Issues

Structure and terminology

9.25 Various submitters raised concerns about the structure of APP 6 and the terminology used. Professor Graham Greenleaf and Mr Nigel Waters noted that the ALRC's Unified Privacy Principle (UPP) 5 provides a single list of 'conditions' on the use or disclosure of personal information, whereas APP 6 splits the list between APP 6(1) and APP 6(2). They expressed concern that this is misleading, as without making it clear that APP 6(2) actually contains exceptions to providing consent for use and disclosure, the principle:

> ...implies that consent has a much more prominent role than it does in reality. Having consent as just one of a number of conditions for use and disclosure in a single clause gives a much more realistic impression of the effect of the law.[28]

9.26 The OPC also commented on the structure of APP 6 and suggested that APP 6(1) and (2) be merged into a shorter simpler single provision.[29] Privacy NSW added that, in its view, APP 6 is too complex and will not assist people in understanding how their personal information may be managed. An alternative form of words for the principle was suggested, providing an initial link to APP 5:

> If an entity has notified an individual about its intended uses or disclosure of personal information it may carry out those uses or disclosures. If an individual has not agreed to those uses or disclosures, the entity may only use or disclose the information if the following circumstances apply:…[30]

Conclusion

9.27 The committee again notes that general comments in relation to the structure of the APPs have been made in chapter 3.

Use or disclosure–APP 6(1)

9.28 APP 6(1) provides that an entity should only disclose personal information about an individual for the 'primary purpose', being the particular purpose for which it was collected. The personal information can only be used or disclosed for a 'secondary purpose' if the individual agrees to the use or disclosure for that purpose, or if one of the exceptions in APP 6(2) applies. The Office of the Guardian for Children and Young People (GCYP) noted its partial support for this provision.[31]

---

28 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10.

29 Office of the Privacy Commissioner, *Submission 39*, p. 32.

30 Privacy NSW, *Submission 29*, p. 4.

31 Office of the Guardian for Children and Young People, *Submission 4*, p. 6.

9.29 The Office of the Information Commissioner, Queensland (OIC), raised concerns that the test allowing the use or disclosure of information is too loose 'as to render the prohibition on secondary use or disclosure meaningless' and went on to state:

> Entities have specific areas of operation which are necessarily both broad albeit concentrated in a specific area...All activities conducted in an entity can be related to all other activities...Under APP6 the potential exists for the secondary use or disclosure of any personal information which in the control or possession of an entity irrespective that the primary purpose is widely different.[32]

9.30 The OIC went on to note that privacy legislation in place in Queensland only allows 'use' for a secondary purpose, and that secondary purpose must be directly related to the primary purpose. According to the OIC, it is determined objectively, rather than subjectively. The OIC suggests that this provision be limited in a similar manner to the Queensland legislation.[33]

9.31 A number of submitters, for example, the Australian Institute of Credit Management (AICM), requested clear guidance as to what might constitute a secondary purpose, as this concept does not appear to be defined within the exposure draft. AICM was concerned that without further clarity regarding the concept of a secondary purpose, use or disclosure of personal information which has a deleterious impact on individuals may occur.[34] These concerns were echoed by the Law Institute of Victoria (LIV), which also called for guidance on the terms 'primary purpose' and 'secondary purpose' to assist entities to adequately comply with the principle. The LIV also noted that such guidance is currently lacking under the NPP as well.[35]

9.32 The Australian Bankers' Association (ABA) noted that unlike NPP 2, APP 6(1) refers to the primary purpose of collection as a 'particular purpose', and this could have implications for the financial services industry:

> The reference to "a particular purpose" should be clear it encompasses all necessary or naturally related purposes. For example, the particular purpose of processing a loan application should include all of the possible activities and use and disclosures of personal information that are necessary to maintain, service and recover the loan. It should be clarified that all necessary or naturally related purposes are able to be described in this way and are taken to be included in the meaning of "particular purpose"... However, compared with the reference to "particular purpose" in APP 6 subsection 7(1), sub-sections 7(2)(h) and (i) suggest that the wider approach

32 Office of the Information Commissioner, Queensland, *Submission 18*, p. 5.

33 Office of the Information Commissioner, Queensland, *Submission 18*, p. 5.

34 Australian Institute of Credit Management, *Submission 8*, p. 3.

35 Law Institute of Victoria, *Submission 36*, p. 6.

> to activities associated with "particular purpose" in the case of financial services might not be available.[36]

9.33 Professor Greenleaf and Mr Waters also suggested changes to the terminology used in this subsection, noting that as an entity may have more than one primary or secondary purpose, the phrases '*a* primary purpose' and '*a* secondary purpose' should be used in place of '*the* primary purpose' and '*the* secondary purpose'.[37]

Conclusion

9.34 The committee notes that the definition of the term 'related', provided in the revised Explanatory Memorandum for the Privacy Amendment (Private Sector) Bill 2000, may assist in the interpretation of the term 'secondary purpose'. The Explanatory Memorandum states:

> To be "related", the secondary purpose must be something that arises in the context of the primary purpose. For example, a business that collects personal information about its clients may use that information to notify its clients of its change of business address.[38]

9.35 The committee notes that the ALRC took such issues into consideration in its report, and formed the view that it is not necessary to require a direct relationship between the primary and secondary purpose with regard to the use and disclosure of non-sensitive information. In fact, the ALRC noted that such a requirement could prove to be significantly onerous for organisations. The ALRC further noted that the removal of the direct relation requirement for the use of non-sensitive information in relation to agencies would be effectively balanced by the introduction of the reasonable expectations test. In summary, the ALRC explained, the:

> ...fact that a primary purpose is related to a secondary purpose increases the likelihood that an individual would reasonably expect his or her personal information to be used or disclosed for that secondary purpose.[39]

9.36 The committee notes concerns about ambiguity of the terms 'primary' and 'secondary' purpose and considers that further guidance on the meaning of these terms would be beneficial.

Exceptions–APP 6(2)

9.37 APP 6(2) provides a list of exceptions to APP 6(1), which allow the use or disclosure of personal information without consent. The ABA welcomed the list of exceptions in AAP 6(2) as practical.[40]

---

36 Australian Bankers' Association, *Submission 15*, pp 7–8.

37 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10.

38 Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*, p. 132.

39 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 851.

Authorised or required by or under Australian law–AAP 6(2)(b)

9.38 Submissions commented on the exception allowing the use or disclosure of personal information where the information is required or authorised by law, or the order of a court or tribunal. Professor Greenleaf and Mr Waters raised concerns that the insertion of the word 'authorised' broadens this exception, and makes its application subjective, as opposed to simply retaining the stricter 'required by law'.[41]

9.39 The Australian Direct Marketing Association and Google argued that the paragraph should be amended to accommodate the requirements of foreign laws, as some companies will be beholden to both Australian law, and the law of other countries in which they carry out business.[42] Google explained:

> For example, a foreign country may mandate disclosure of personal information in response to a subpoena issued by a court exercising jurisdiction over the operations of the service provider in that foreign country. It would be inappropriate to place the service provider in jeopardy under Australian law for responding to valid court process in a foreign jurisdiction.[43]

Conclusion

9.40 Similar concerns were taken into consideration in the ALRC's review; however, the ALRC did not deem it appropriate to further restrict this exception. The committee notes that the ALRC recommended certain safeguards pertaining to this exception, including that agencies and organisations must be able to provide the basis on which they claim the exception by naming the law which requires or authorises the use or disclosure.[44] The committee notes that the Government supported the retention of this exception in its response.[45]

9.41 As discussed in previous chapters, the committee notes that the provisions in the current Privacy Act which provide that acts or practices undertaken outside of Australia which are required by 'an applicable law of a foreign country' will not be taken as a breach of privacy, will be replicated in the new Privacy Act.[46]

---

40 Australian Bankers' Association, *Submission 15*, p. 7.

41 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 7 and 10.

42 Australian Direct Marketing Association, *Submission 27*, p. 9; Google Australia Pty Limited, *Submission 16*, p. 7.

43 Google Australia Pty Limited, *Submission 16*, p. 7.

44 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 863–866.

45 Australian Government, *Enhancing National Privacy Protection*, p. 52.

46 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 7.

Serious threat to life, health or safety–APP 6(2)(c)

9.42 Concerns were raised that the exception allowing the use or disclosure of personal information to lessen or prevent a serious threat to the life, health or safety of the public or an individual has been significantly expanded. Professor Greenleaf and Mr Waters noted there is no reference to a requirement for any threat to be 'imminent', and threats to the health and safety of individuals and the public have been added. Further, they argued that the condition that it be 'unreasonable or impracticable to obtain consent' is quite weak, and that it should be replaced with a stronger provision that it be physically or legally impracticable to obtain consent.[47]

9.43 The Australian Medical Association (AMA) also commented on the removal of the word 'imminent', and was concerned to ensure that patient privacy is not breached as a result of this change. The AMA submitted that guidance on what effect the change in wording will have in practice, specifically how the provision differs from the current requirement, and guidance on when it is appropriate for a doctor to disclose a patient's personal information without consent, will be required.[48]

9.44 Qantas raised concerns about the use of the term 'serious' and recommended that the term be removed from throughout the exposure draft, as 'The question of "*seriousness*" will always be subjective'. Therefore Qantas suggested that the following form of words would be more appropriate for the exception: 'the entity reasonably believes that the use or disclosure will lessen or prevent a threat'.[49]

9.45 While the Health Services Commissioner, Victoria (HSC) broadly supports APP 6 as consistent with the *Health Records Act 2001* (Vic), it was noted that APP 6(2)(c)(ii), may limit the ability of an entity to use or disclose personal information of an individual suffering from psychiatric illness. The HSC suggested that the appropriateness of this provision, with regards to health privacy, be considered.[50]

Conclusion

9.46 The committee notes the ALRC's considerations regarding the use of the terms 'imminent' and 'serious'. In particular, the committee observes that the removal of the term 'imminent' simply removes the need to assess the immediacy of the threat. However, the retention of 'serious' ensures that an assessment of the gravity of the potential outcome of a threat is assessed before a use or disclosure is made.[51]

---

47 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 7 and 10.

48 Australian Medical Association, *Submission 37*, p. 2.

49 Qantas, *Submission 38*, pp 4–6.

50 Health Services Commissioner, Victoria, *Submission 26*, p. 3.

51 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 859–60.

9.47 The committee also observes that the Government noted such concerns in its response to the ALRC report. While the Government agreed with the removal of the term 'imminent', it acknowledged concerns that the removal of the term broadened the exception. To address these concerns, the Government proposed the addition of a requirement that it be 'unreasonable or impracticable' to obtain an individual's consent to a use or disclosure for this purpose.[52] The committee notes that this has been taken into account in the exposure draft.

9.48 The committee notes the concerns of the Health Services Commissioner and suggests that the circumstances of individuals with psychiatric illness be taken into consideration.

Unlawful activity–AAP 6(2)(d)

9.49 The Law Council of Australia and the Australian Direct Marketing Association (ADMA), expressly supported the inclusion of a provision permitting disclosure and use of personal information in circumstances of suspected unlawful activity or misconduct of a serious nature. The Law Council of Australia noted that the absence of such a provision in NPP 2 has caused organisations significant issues to date.[53]

9.50 Various submitters noted concern about the limited application of APP 6(2)(d)(i), and argued that entities should have more discretion regarding disclosures in respect of potential unlawful activity or serious misconduct. The Financial Services Council (FSC) and ABA suggested that entities should also have some discretion to disclose information about any potential unlawful activity or serious misconduct, even if it doesn't directly relate to their own functions or activities.[54]

9.51 In contrast, Professor Greenleaf and Mr Waters argued that this provision is not necessary, and could be used to compile and maintain 'blacklists' simply based on suspicion of wrongdoing, with no requirement that any such listed individuals be afforded natural justice. Should this provision be retained, they suggested that the exception should be conditional on the entity undertaking 'appropriate action', within a reasonable period of time, to prevent the creation of 'blacklists'.[55]

9.52 In its response to these matters, the Department of the Prime Minister and Cabinet (the department) noted that while the use and disclosure of personal information is permitted for any unlawful activity relating to the entity's functions or

---

52 Australian Government, *Enhancing National Privacy Protection*, pp 54–55.

53 Law Council of Australia, *Submission 31*, p. 5; Australian Direct Marketing Association, *Submission 27*, p. 10.

54 Qantas, *Submission 32*, p. 6; Australian Bankers' Association, *Submission 15*, p. 8; Financial Services Council, *Submission 34*, p. 2.

55 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 7 and 10.

activities, the use and disclosure of personal information should not be permitted merely for minor breaches of misconduct. The department further commented that these are issues that can be handled internally by the entity without the need to use or disclose an individual's personal information. The department concluded:

> Consistent with the ALRC's views, the exception is aimed at internal investigations by an entity about activities within or related to that entity. If an entity believed that there was unlawfulness not related to its own functions and activities, it may be possible to disclose the information under the law enforcement exception in APP 6(2)(e).[56]

Conclusion

9.53 The committee notes concerns about the application of this exception. However, the Government response makes it clear that the inclusion of an exception allowing the use or disclosure of personal information where unlawful activity or serious misconduct is suspected was supported.[57] Further, the department has noted that the intention of the provision is that it will only be applied to the internal investigations of an entity.

Enforcement related activities–AAP 6(2)(e)

9.54 Professor Greenleaf and Mr Waters noted that while they believe this provision is necessary, they are concerned that the exception allowing the use and disclosure of personal information for the enforcement activities of an enforcement body has been expanded, and subsequently weakened.[58]

9.55 The committee observes that the Government supported the inclusion of an exception allowing the use or disclosure of personal information for law enforcement activities in its response to the ALRC report.[59]

Diplomatic or consular functions–APP 6(2)(f)

9.56 Concerns were raised by Professor Greenleaf and Mr Waters regarding the exception allowing the use or disclosure of personal information for an agency's diplomatic or consular functions or activities. They argued that this new 'special pleading' provision allows the diplomatic services to use or disclose personal information based solely on the entity's own 'reasonable belief'. They submitted that 'any case for additional exceptions should be argued rather than simply asserted'.[60]

---

56 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 16.

57 Australian Government, *Enhancing National Privacy Protection*, p. 52.

58 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 8 and 10.

59 Australian Government, *Enhancing National Privacy Protection*, p. 52.

60 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 8 and 10.

9.57 The Office of the Victorian Privacy Commissioner (Privacy Victoria) noted that the exceptions provided for in APP 6(2)(f) and (g) relate solely to Commonwealth agencies. Privacy Victoria argued that given the APPs are supposed to be simple and high-level, such express detail reduces the clarity of the APPs and the ability of States and Territories to readily adopt them with little amendment.[61] The committee's comments in relation to agency specific exceptions are canvassed in chapter 3.

Missing person–APP 6(2)(g)

9.58 APP 6(2)(g) provides an exception in relation to the use and disclosure of personal information where it would assist to locate a person who has been reported missing.

9.59 In its submission to the committee, the ALRC noted that the issue of disclosure of personal information regarding missing persons has been dealt with differently in the exposure draft than recommended by the ALRC in its report. The ALRC explained that the matter was canvassed in its Issues Paper, and while some stakeholders supported disclosure of information in such a situation, there was concern among others that a missing person may not wish to be found. Therefore, to 'create a general exception in respect of all missing person investigations risks interfering with the privacy of certain missing individuals and, possibly, endangering their lives'.[62] The ALRC concluded that:

> ...the privacy principles did not need to be amended expressly to allow agencies and organisations to use or disclose personal information to assist in the investigation of missing persons, given that other proposed principles should facilitate the disclosure of information in appropriate circumstances (e.g. in relation to serious threats to a person's life, health or safety).[63]

9.60 Given that an exception regarding missing persons has been included in the exposure draft of the APPs, the ALRC emphasised that the Australian Privacy Rules proposed under section 21 of the exposure draft will be important in providing the required constraints relating to the collection and use of personal information to assist in the location of a missing person.[64]

9.61 Professor Greenleaf and Mr Waters also commented on the use of Privacy Rules in relation to this exception and argued that guidelines pertaining to this principle should be included in the APP itself, and not left to regulations.[65]

---

61 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 7.

62 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 874.

63 Australian Law Reform Commission, *Submission 1*, pp 1–2.

64 Australian Law Reform Commission, *Submission 1*, pp 2–3.

65 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 8 and 10.

9.62 The Office of the Guardian for Children and Young People (GCYP) expressed concern that a missing person may not wish to be located for a number of reasons, including for fear for their personal safety. The GCYP argued that APP 6(2)(g)(i) is very broad, and that a 'clear definition and procedure to test validity of an assumption that someone is "missing" is required.'[66]

Conclusion

9.63 The committee observes that the Government provided a detailed explanation in its response to the ALRC's recommendations for its decision to include an exception for the use and disclosure of information to assist in locating missing persons. The Government acknowledged that in some cases a missing person may not wish to be located. For this reason, the Government has noted its intention to have binding rules for the use of this exception issued by the Privacy Commissioner, covering a series of matters, including that any use or disclosure should not go against 'any known wishes' of the individual, that an assessment of whether the use or disclosure will pose a serious threat to the individual be undertaken, and that any use or disclosure of personal information should be limited. The Government has indicated that these rules will be a legislative instrument and will therefore be subject to parliamentary scrutiny.[67]

9.64 The intentions the Government signalled in its response to the ALRC report were implemented in the exposure draft. As explained in the Companion Guide, this exception will only be able to be used in accordance with the rules issued by the Commissioner, as 'it is important that the permission to collect, use or disclose personal information strikes the right balance, ensuring that persons who have intentionally chosen to discontinue contact remain undisturbed'.[68]

9.65 The committee considers that the use of this exception, subject to rules issued by the Australian Information Commissioner, will provide adequate protection for those who do not wish to make contact with the people who are looking for them and, at the same time, assist in those cases where the use and disclosure of personal information is needed to locate genuinely missing people.

Legal or equitable claim and alternative dispute resolution process–APP 6(2)(h) and (i)

9.66 In its submission GCYP requested clarification of the scope of APP 6(2)(h), relating to the use or disclosure of personal information for the purposes of a legal or equitable claim, noting that agencies are already required to provide information to the judiciary in certain circumstances. GCYP went on to state that these legal

66 Office of the Guardian for Children and Young People, *Submission 4*, p. 6.

67 Australian Government, *Enhancing National Privacy Protection*, p. 53.

68 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 16.

requirements, in conjunction with the other provisions in APP 6, give sufficient provision for disclosure without the inclusion of this paragraph.[69]

9.67 Professor Greenleaf and Mr Waters further noted that APP 6(2)(h) does not require any assessment of how trivial a 'legal or equitable claim' may be in comparison with the impact that disclosure or use of information for such a claim may have on an individual's privacy.[70]

9.68 The Law Council of Australia noted concern that APP 6(2)(h) and (i) are not broad enough to adequately cover 'all disputes before alternative dispute resolution bodies, tribunals or external dispute resolution schemes'. Consequently, the Law Council suggested that if an entity believes use or disclosure of personal information is reasonably necessary for the purposes of a dispute before any such body, use or disclosure should be allowed under the principle.[71]

9.69 Professor Greenleaf and Mr Waters suggested that the word 'prescribed' be inserted into APP 6(2)(i) to ensure that only genuine alternative dispute resolutions qualify under this exception.[72]

Conclusion

9.70 The committee supports the inclusion of the exceptions for legal or equitable claims and alternative dispute resolution (ADR). The committee considers that guidance from the Australian Information Commissioner will be necessary to clarify the operation of these provisions and, in particular, to address concerns such as those raised by the Law Council of Australia that APP 6(2)(h) and (i) are not broad enough to adequately cover 'all disputes before alternative dispute resolution bodies, tribunals or external dispute resolution schemes'.

9.71 In relation to ADR, the committee notes that the ALRC recommended a confidentiality safeguard to limit the scope of the exception regarding ADR, and given this, the ALRC considered it unnecessary to provide any further stipulation on the ADR process used, noting it could prove problematic, as such a limitation could 'artificially fragment the application of the exceptions'. The ALRC further noted:

> ...by its very nature, ADR is dynamic and diverse. Provided the confidentiality safeguards outlined above are in place, this diversity should be accommodated. This is best managed by applying the exception to the broad ambit of ADR processes.[73]

---

69 Office of the Guardian for Children and Young People, *Submission 4*, p. 6.

70 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10.

71 Law Council of Australia, *Submission 31*, pp 5–6.

72 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 10.

73 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1492–93.

9.72 The committee observes that the Government supported the inclusion of an exemption for ADR processes in its response to the ALRC report, and encouraged the development of appropriate guidance by the Privacy Commissioner.[74]

Additional exception

9.73 Qantas argued for an additional exception in relation to emergencies or disasters. Qantas noted that under Part VIA of the current Privacy Act, in the event of a situation declared an emergency or disaster by the Prime Minister, certain personal information is allowed to be collected, used and disclosed, and that this provision is to be replicated in the new Privacy Act. However, Qantas was concerned that some emergency or disaster situations which do not warrant a Prime Ministerial declaration, may still result in significant injuries and it may be considered desirable to release personal information to authorities in such instances. Consequently, Qantas suggested that an exception be included in the legislation, allowing the disclosure or use of personal information if, 'in the reasonable opinion of the entity, it is necessary for or will assist in an appropriate response to an emergency or disaster.'[75]

9.74 The committee notes that following the introduction of Part VIA of the current Privacy Act in 2006, the ALRC observed that stakeholders have indicated that 'most, if not all, of the problems arising from the handling of personal information in emergency situations have been dealt with adequately by the advent of Part VIA.'[76]

9.75 The Companion Guide states that it is expected that Part VIA of the current Privacy Act will be replicated in the new Privacy Act. The committee notes the explanation by the ALRC in its report, which indicated that the provisions in the privacy principles will apply to 'emergencies or other threats to life that are not declared under Pt VIA, or the subject of a TPID' [temporary public interest determination].[77] The committee considers that it appears this is the function of APP 6(2)(c).

Written note of use or disclosure–APP 6(3)

9.76 GCYP noted in-principle support for this section, which requires a written note of the use or disclosure of personal information for enforcement activities permitted under APP 6(2)(e). However, GCYP requested guidance on what constitutes a written note of use or disclosure, and requirements for secure record keeping. GCYP also suggested that the following information should be included in any such note:

---

74 Australian Government, *Enhancing National Privacy Protection*, p. 82.

75 Qantas, *Submission 38*, p. 6.

76 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1511.

77 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 6; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 853.

- if consent was sought
- reasons for overriding the client's wishes or for not seeking consent
- advice disclosed, received or requested from others
- reasons for not agreeing to an information sharing request
- what information was collected, disclosed, with whom, and for what purpose
- any follow up activity required by the organisation or entity.[78]

9.77 Professor Greenleaf and Mr Waters suggested that the requirement to provide a written note should extend to paragraphs (2)(d), (f) and (g) as well, as they are similar to (2)(e).[79] Privacy NSW went further, and suggested that this requirement be extended to any use or disclosure of personal information for a secondary purpose.[80]

9.78 The department, in responding to these suggestions, noted that the ALRC had found that imposing a general legislative requirement to log use and disclosure is, on balance, untenable. It noted that the sheer volume of use and disclosure of personal information by agencies and organisations on a daily basis would render such a requirement impractical, costly and onerous. However, the ALRC believed there was considerable merit in imposing such a requirement in the special context of law enforcement. Further, while there is an argument that the unlawful activity exception in APP 6(2)(d) is similar to the law enforcement exception, the ALRC noted that this potential overlap made it seem unnecessary for the Privacy Act to require the logging of all use and disclosure under the unlawful activity exception.[81]

Conclusion

9.79 The committee concludes that there is no reason to extend the provisions of APP 6(3) to include other exceptions.

Exceptions–APP 6(5)

9.80 APP 6(5) provides that use and disclosure of government related identifiers and personal information for the purposes of direct marketing are not subject to APP 6. The GCYP noted its support for this provision.[82] However, Professor Greenleaf and Mr Waters argued that this is a significant departure from the ALRC's recommendations, and from the NPPs. They submitted that the direct marketing and government identifier provisions were not designed as 'standalone' principles, as reflected in:

78 Office of the Guardian for Children and Young People, *Submission 4*, p. 6.

79 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 11.

80 Privacy NSW, *Submission 29*, p. 4.

81 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 16.

82 Office of the Guardian for Children and Young People, *Submission 4*, p. 6.

> ...the ALRC's recommendations (UPPs 5, 6 & 10) and the existing NPPs 2 & 7, which have direct marketing and identifier principles as 'extra requirements' applying over and above the normal application of the use and disclosure principle (to the extent that they are compatible).[83]

9.81 This argument was supported by Qantas Airways Limited, and is further examined in chapter 10.[84]

9.82 However, Professor Greenleaf and Mr Waters suggests that if the direct marketing and government identifier provisions are maintained as separate principles, APP 6(5) should provide a clearer link to these separate principles.[85]

83 Professor G Greenleaf &Mr N Waters, *Submission 25*, p. 11.

84 Qantas, *Submission 38*, pp 6–7.

85 Professor G Greenleaf &Mr N Waters, *Submission 25*, p. 11.

Chapter 10

Australian Privacy Principle 7–direct marketing

Introduction

10.1 Australian Privacy Principle (APP) 7 addresses significant community concern about the use and disclosure of personal information for direct marketing. It provides limitations on organisations which use or disclose personal information for such purposes.[1]

10.2 The Companion Guide noted that the language in the draft principle differs to the approach outlined in the Government's first stage response to the Australian Law Reform Commission (ALRC) report. Where the Government response referred to 'existing customers' and 'non-existing customers', the exposure draft refers to individuals who have directly provided information to the entity undertaking direct marketing and individuals who have not directly provided their personal information to the entity. The Companion Guide explains that while the language differs, the same policy is achieved.[2]

Background

What is direct marketing?

10.3 Direct marketing is not currently defined under the *Privacy Act 1988* (Privacy Act). Differing descriptions have been provided by the Office of the Privacy Commissioner (OPC) and the Australian Direct Marketing Association (ADMA). The ALRC described direct marketing as follows:

> 'Direct marketing' involves the promotion and sale of goods and services directly to consumers. Direct marketing can include both unsolicited direct marketing and direct marketing to existing customers. For unsolicited direct marketing, direct marketers usually compile lists of individuals' names and contact details from many sources, including publicly available sources. An individual may not always know that his or her personal information has been collected for the primary purpose of direct marketing. Direct marketing to existing customers may involve communications designed to let customers know about new products or services.[3]

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

2 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 889–90.

10.4 This appears to be the same basic meaning adopted in the Companion Guide, which describes the practice as the promotion or sale of goods or services directly to individuals.[4]

10.5 The ALRC noted that while some stakeholders had called for a definition of direct marketing to be provided in the Privacy Act, the term seems to be generally understood, and 'there is no consensus about how the term should be defined'. The ALRC formed the view that the term should not be defined for the purposes of the Privacy Act, as providing a definition of direct marketing may limit the application of the principle:

> For example, if direct marketing is defined by reference to current practice, but practice later evolves, new methods of direct marketing may not be caught by the definition and so would not be subject to the 'Direct Marketing' principle.[5]

Current provisions regarding direct marketing

10.6 While there is no explicit provision relating to direct marketing by agencies under the Information Privacy Principles (IPPs), National Privacy Principle (NPP) 2.1(c) allows the use of personal information by organisations for the *secondary* purpose of direct marketing, subject to a list of conditions.[6]

10.7 Further, in its report, the ALRC noted that there are other exceptions under the NPPs which permit the use or disclosure of information for direct marketing, for example if the individual has consented to the use or disclosure, or if the information was collected for the *primary* purpose of direct marketing, etc. If use or disclosure of personal information is permitted under an exception due to collection of information for the *primary* purpose of direct marketing, that use or disclosure is not subject to the list of conditions under NPP 2.1(c).[7]

Reviews direct marketing provisions

10.8 The practice of direct marketing, unsolicited direct marketing communications in particular, is the subject of considerable community concern. A series of issues have been identified regarding the operation and application of the principles regarding direct marketing. Some of these issues were considered in the Office of the Privacy Commissioner's (OPC) report *Getting in on the Act: The Review*

---

4 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 898.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 891–92.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 891–93.

of the Private Sector Provisions of the Privacy Act 1988 (OPC review).[8] Concerns regarding the direct marketing provisions were also examined as part of the 2005 Senate Legal and Constitutional Affairs References Committee inquiry into the *Privacy Act 1988*.[9]

10.9 The ALRC review considered the following matters:

- whether the privacy principles should regulate direct marketing regardless of whether the personal information in question was collected for a primary or secondary purpose of direct marketing;
- whether direct marketing should be regulated by a separate privacy principle;
- whether the Privacy Act should regulate direct marketing by agencies;
- how the 'Direct Marketing' principle in the Privacy Act should relate to other legislation that deals with particular forms of direct marketing; and
- the content of the 'Direct Marketing' principle and the need for guidance from the OPC in relation to the 'Direct Marketing' principle.[10]

Direct marketing as a primary or secondary purpose, and a discrete principle

10.10 A chief concern appears to be the different requirements for the use or disclosure of information for the purposes of direct marketing depending on whether the direct marketing is the primary purpose of collection, or a secondary purpose. The ALRC explained that 'there is currently considerable ambiguity about whether organisations have collected personal information for the primary or secondary purpose of direct marketing'.[11]

10.11 The OPC review noted this is of particular concern, because an individual is unlikely to comprehend the implications of the differences between collection for a primary purpose and a secondary purpose. This is aptly illustrated by the following example:

> ...an organisation may run a competition for the primary purpose of collecting information; awarding prizes to successful entrants being a secondary purpose. The individual, on the other hand, may assume that the purpose of the competition is to provide an opportunity to consumers to win

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 889–95; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, pp 94-103.

9 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, pp 81–87 and 158.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 891.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 891–95.

> prizes. Even if he or she reads the fine print, an individual is unlikely to draw a distinction between a primary and a secondary purpose and to understand the consequences of the distinction.[12]

10.12 The ALRC noted that while some forms of direct marketing can be harmful to the privacy of individuals, if conducted appropriately, direct marketing can also offer benefits. After considering the concerns addressed in previous reviews, and those raised by stakeholders, the ALRC recommended that regulation of direct marketing should be provided for through a single discrete privacy principle. Importantly, the principle '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' and 'should distinguish between direct marketing to individuals who are existing customers and direct marketing to individuals who are not existing customers'.[13]

Application to agencies

10.13 Agencies are currently not subject to express regulation of direct marketing under the IPPs. In considering whether the direct marketing principle should apply to agencies, the ALRC looked at what is encompassed by the term 'agency' in some detail, and came to the understanding 'that "agency" will not generally include Commonwealth, state or territory commercial enterprises which are in competition with private sector organisations'.[14] The ALRC further noted that while agencies are generally exempt from direct marketing requirements under the Privacy Act, according to the policy position expressed by the Government:

> ...even if legislation technically does not apply to government bodies who are in competition with the private sector, it will be best practice for such government bodies to meet legislative requirements in relation to those commercial activities.[15]

10.14 The ALRC formed the view that the direct marketing principle should not apply to agencies as it may impact on the ability of agencies to communicate legitimate and important information to individuals. However, the ALRC supported Government policy in relation to government bodies engaged in commercial activities.[16]

---

12 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, p. 95.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 897–98.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 899–903.

15 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 899–900.

16 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 902–03.

Interaction with other legislation

10.15 The ALRC noted the existence of sectoral legislation which relates to specific types or aspects of direct marketing, such as the *Do Not Call Register Act 2006* (DNCR Act) which regulates some aspects of telemarketing and the *Spam Act 2003* (Spam Act) which regulates some aspects of email marketing. The ALRC noted that:

> ...there is a strong community view that some forms of direct marketing are, or have the capacity to be, more intrusive than others. Clearly, those forms of direct marketing should be subject to regulation that differs from the rules applicable to less intrusive forms of direct marketing.[17]

10.16 In light of this, the ALRC formed the view that the privacy principles should provide for 'the generally applicable requirements for organisations engaged in the practice of direct marketing.' However, the requirements under the direct marketing privacy principle 'should be able to be displaced by more specific legislation that deals with a particular type of direct marketing, or direct marketing by a particular technology'.[18]

Existing and non-existing customers concept

10.17 The ALRC recommended that the direct marketing principle should distinguish between direct marketing to individuals who are existing customers and those who are non-existing customers. This reflects the concept of existing relationships which is used to define consent in the Spam and DNCR Acts. It also addresses stakeholder comments that 'direct marketing to existing customers is a legitimate business activity and is acceptable where it is within the reasonable expectations of such customers'.[19]

10.18 However, the ALRC specified that the use or disclosure of personal information for the purposes of direct marketing to existing customers should only take place where the customer would reasonably expect the use or disclosure of their information for that purpose. This concept of reasonable expectation already exists under the current Privacy Act.[20]

10.19 The ALRC considered that the requirements applying to the use or disclosure of personal information for direct marketing to non-existing customers should be more onerous than those applying to the use or disclosure of personal information for direct

---

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 905.

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 905–906.

19 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 906–912.

20 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 906–912.

marketing to existing customers. The ALRC suggested that personal information of non-existing customers should only be used or disclosed for the purposes of direct marketing if 'the individual has consented; or the information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure'.[21]

10.20 The ALRC considered that guidance on the following matters would be required from the OPC:

- what constitutes an existing customer;
- the types of direct marketing communications which are likely to be within the reasonable expectations of existing customers and the extent to which the use and disclosure of sensitive information for the purposes of direct marketing will be within an existing customer's reasonable expectations; and
- the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing.[22]

Opt-in requirement vs opt-out requirement

10.21 The Senate Legal and Constitutional Affairs References Committee inquiry into the *Privacy Act 1988* recommended the consideration of providing an 'opt-in' requirement for direct marketing, in line with the Spam Act. The OPC review took a different approach, recommending that consideration be given to amending the Privacy Act to grant consumers the option to 'opt-out' of direct marketing at any time, and that organisations should be required to comply with such a request within a particular timeframe.[23]

10.22 The ALRC noted that the majority of stakeholders supported the adoption of an 'opt-out' regime in relation to direct marketing, however recommended a distinction be drawn between direct marketing to non-existing customers and direct marketing to existing customers. Non-existing customers should be provided with an opportunity to opt-out of direct marketing in every direct marketing communication. However, in relation to existing customers, the ALRC considered it sufficient to make the customer

21 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 911.

22 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 928.

23 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 912; Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, pp 81–87 and 158; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, p. 103.

aware through the organisation's privacy policy, that they are able to opt-out of direct marketing at any time.[24]

Direct marketing to minors

10.23 The ALRC considered it appropriate that parental consent should be required before the use or disclosure of the personal information of a child or young person under the age of 15 for the purposes of direct marketing is permitted. Further, the ALRC considered that a child or young person under the age of 15 should always be treated as a non-existing customer, ensuring that stricter obligations relating to the use or disclosure of their personal information for the purposes of direct marketing apply. The ALRC suggested that:

> ...direct marketing to individuals under the age of 15 years can only occur where either: the individual has consented; or the information is not sensitive information, and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure.[25]

Providing the source of information

10.24 The OPC review recommended that the Privacy Act be amended to 'require organisations to take reasonable steps, on request, to advise an individual where it acquired the individual's personal information.'[26] This recommendation was supported by the Senate Legal and Constitutional Affairs References Committee.[27]

10.25 The ALRC noted support from stakeholders for such a requirement as this would enable individuals to assert their privacy rights regarding direct marketing. However, the ALRC was conscious that this requirement might increase the compliance burden on organisations, and suggested the requirement be limited to individuals who are non-existing customers, and that a 'reasonable and practicable' test be introduced, to ensure that the requirement would not be overly onerous for organisations to comply with. It was suggested that the OPC could provide guidance on the factors to be considered in determining whether it is 'reasonable or practicable' to advise an individual of the source of information. The ALRC also considered that the 'source' in this requirement should refer to 'the direct source from which the organisation acquired the information' as opposed to the original source of information. The ALRC stated that:

---

24 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 915.

25 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 917.

26 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, p. 103; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 921.

27 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, p. 158.

> It would be unduly onerous to require organisations to track personal information back to the original source. In some cases, organisation C may not be aware that organisation B obtained the personal information from some other source.[28]

Government response

10.26 The Government agreed that provisions regulating the use and disclosure of personal information for the purposes of direct marketing should form a separate and discrete principle. The Government further agreed that different standards should be applied to those who have an existing relationship with an organisation and those who do not. However, the appropriateness of the term 'customer' was questioned, and the Government stated it would seek advice from the OPC to ensure that the draft legislation reflects the correct intent.[29]

10.27 In relation to extending the application of the principle to agencies, the Government stated that this 'would generally not be appropriate' and noted that section 7A of the existing Privacy Act provides for the treatment of acts of certain agencies as acts of organisations. A note should be added to the principle to draw attention to section 7A.[30]

10.28 The Government agreed that specific sectoral legislation such as the Spam and DNCR Acts should displace the more general requirements under the direct marketing principle.[31]

10.29 In relation to sensitive information, the Government took a different position to the ALRC and stated that an individual's consent should always be sought for the use and disclosure of sensitive information for the purposes of direct marketing, regardless of whether the individual is an existing or non-existing customer.[32]

10.30 The response noted the Government's agreement with the recommendation that personal information of existing customers should only be used or disclosed for the purpose of direct marketing if the individual would reasonably expect the organisation to use or disclose their information for that purpose, and if the organisation provides the individual with a simple and functional way of opting-out of direct marketing communications. The Government also concurred with the ALRC's suggestion that in every direct marketing communication, non-existing customers

---

28 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 925–926 and 928.

29 Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, p. 56.

30 Australian Government, *Enhancing National Privacy Protection*, p. 56.

31 Australian Government, *Enhancing National Privacy Protection*, p. 57.

32 Australian Government, *Enhancing National Privacy Protection*, p. 57.

should be informed of their ability to opt-out of direct marketing communications, and that a simple and functional means of opting-out should be offered.[33]

10.31 The Government also recognised concerns regarding the potential effect of direct marketing on children, in particular direct marketing via email and SMS which are regulated under the Spam Act. It was noted that, in effect, the provisions under the Privacy Act principally relate to postal direct marketing and there is 'insufficient evidence that postal direct marketing to young people has resulted in substantial adverse consequences'. Given this, and given that determining the age of an individual is likely to result in organisations collecting more information about individuals than would otherwise be necessary, the Government did not agree that different standards for the use and disclosure of personal information for the purpose of direct marketing should be applied on the basis of an individual's age. In the Government's view this would only 'impose an unnecessary regulatory burden and added complexity, without substantial benefit'.[34]

10.32 Finally, the Government agreed that, where practicable, an organisation should be obliged to advise an individual of the source from which they obtained the individual's information, if this information is requested by the individual.[35]

Issues

10.33 The committee received many comments in relation to structure and terminology used and submitters commented that APP 7 is a particularly difficult and complex principle. Submitters also noted that the requirements under APP 7 would be administratively burdensome and costly to comply with, particularly as it will require investment in IT infrastructure and other systems.[36]

Structure and terminology

10.34 A number of submissions raised concerns about the complexity and structure of APP 7. While the National Australia Bank (NAB) and the Australian Bankers' Association (ABA) supported a separate principle for direct marketing, a larger number of submitters did not. They suggested that APP 7 be incorporated into APP 6 to ensure clarity and avoid confusion.[37] Privacy NSW further suggested that if this was to occur, APP 7(1)-(6) should be contained in an Australian Privacy Rules.[38]

---

33 Australian Government, *Enhancing National Privacy Protection*, pp 57–58.

34 Australian Government, *Enhancing National Privacy Protection*, pp 57–58.

35 Australian Government, *Enhancing National Privacy Protection*, p. 59.

36 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 1; Westpac Group, *Submission 13*, p. 2.

37 National Australia Bank, *Submission 2*, p. 4; Australian Bankers' Association, *Submission 15*, p. 8; Privacy NSW, *Submission 29*, pp 4–5; Australian Privacy Foundation, *Submission 33*, p. 2; Qantas, *Submission 38*, p. 7.

38 Privacy NSW, *Submission 29*, pp 4–5.

10.35 Another view was put by Dr Colin Bennett who commented that direct marketing is a practice, rather than a principle and 'to elevate the practice (and industry) to the statues of a principle is really inconsistent with other "principle" based laws and regimes and will be viewed as such by overseas privacy regulators and experts'.[39]

10.36 Submitters also commented about the complexity of the principle and called for guidance and clarity around the operation or meaning of certain parts of the provision.[40] The OPC commented that 'if direct marketing is to be addressed in a separate principle, it is important that the principle be clearly drafted, easily understood, and proportionate with community expectations'.[41]

10.37 Privacy Law Consulting Australia also noted that complexity of structure is a particular concern, as the principle is difficult to understand and apply. Consequently, organisations will experience difficulty in developing compliance programs and systems which meet the legislative requirements. Privacy Law Consulting Australia stated:

> This could result in, for example, organisations simply adopting "the lowest common denominator" (e.g. providing opt-out facilities and/or obtaining consent) in relation to all direct marketing activities, which may be unintended consequences of the principle.[42]

10.38 The Department of the Prime Minister and Cabinet (the department) commented on the matters raised by Privacy Law Consulting Australia and stated that the requirements in APP 7 are intended to allow organisations to undertake legitimate direct marketing activities subject to strict rules aimed at protecting individuals from having their personal information used and disclosed inappropriately. Organisations will be required to consider their existing procedures to ensure that they comply with the new regime.[43]

10.39 The department also commented that the Government had agreed to a separate principle for direct marketing to provide 'greater clarity' and went on to note the ALRC's comments that 'stakeholder concerns regarding the direct marketing activities of some organisations were unlikely to be addressed adequately if the relevant privacy

---

39 Dr Colin Bennett, *Submission 11*, p. 3.

40 See National Australia Bank, *Submission 2*, p. 4; Epworth HealthCare, *Submission 9*, p. 1; Privacy Law Consulting Australia, *Submission 24*, p. 5; Professor G Greenleaf & Mr N Waters, Submission *25*, p. 11; Australian Direct Marketing Association, *Submission 27*, p. 2; Australian Privacy Foundation, *Submission 33*, p. 2; Financial Services Council, *Submission 34*, pp 2–3; Law Institute of Victoria, *Submission 36*, p. 6; Qantas, *Submission 38*, p. 7.

41 Office of the Privacy Commissioner, *Submission 39*, p. 32.

42 Privacy Law Consulting Australia, *Submission 24*, p. 4.

43 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 21.

principle only covered secondary purpose direct marketing (as existing NPP 2.1 does)'.[44]

10.40 Submitters commented on the drafting of this principle, noting that the inconsistent use of terminology and positive and negative expression of requirements. Submitters also noted that the headings in APP 7(2) and APP 7(3) do not adequately reflect the intent and content of the provisions, and should be redrafted.[45] The Australian Institute of Credit Management suggested that APP 7(2)(d) is not clear and could be redrafted to set out a 'logical process of receipt and opting-out'.[46]

10.41 Professor Greenleaf and Mr Waters commented on the 'poor' drafting in that it does not use the same distinctions as are explained in the Companion Guide.[47] These issues combined with the use of cross-referencing have made the relationship between provisions very unclear. They commented, for example, that APP 7(1)(b) is expressed as an exemption to APP 7(1), is subject to two pre-conditions, and requires readers to refer to other provisions before understanding where it applies. Further, APP 7(2) and (3) are in fact exceptions to APP 7(1), however, this is not clear from the structure or the drafting of the principle, and consequently 'APP 7 fails the fundamental test that legal obligations should be at least reasonably comprehensible'. It was submitted that the principle would be better constructed as a set of 'conditions' on direct marketing activity and could be modelled on UPP 6.[48]

10.42 The OPC concluded:

> The principle's structure could be simplified and reorganised to reflect the general rules that regulate how information can be used or disclosed for direct marketing, followed by exceptions (such as for contracted service providers) and any additional requirements.[49]

Conclusion

10.43 In relation to the comments that direct marketing should not be a separate privacy principle, the committee notes the comments of the ALRC which reported that stakeholders had submitted both in favour of, and against the creation of a discrete principle on direct marketing. The ALRC report provided the following rationale for its recommendation for a separate principle, and this was supported by the Government response:

---

44 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 17.

45 Australian Direct Marketing Association, *Submission 27*, pp 5–6; Office of the Privacy Commissioner, *Submission 39*, pp 32-34.

46 Australian Institute of Credit Management, *Submission 8*, pp 3–4.

47 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 12.

48 Privacy Law Consulting Australia, *Submission 24*, p. 4; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 12.

49 Office of the Privacy Commissioner, *Submission 39*, p. 33.

> Making clear that the 'Direct Marketing' principle in the Privacy Act sets out the general requirements in this area, and that these may be displaced by other requirements in certain contexts, where Parliament deems it appropriate, allows for a regime that is more responsive to the specific needs of consumers and business.[50]

10.44 However, as the ALRC concluded that any provisions relating to use or disclosure of information for direct marketing should apply regardless of whether the information was collected for the primary or secondary purpose of direct marketing, it should be constituted as a separate principle to the general 'use and disclosure' principle. In its response to the ALRC report, the Government supported the creation of a discrete principle regulating the use and disclosure of personal information for the purposes of direct marketing.[51] The committee also notes the department's comments regarding a separate principle and supports this approach.

10.45 The committee considers that, as currently drafted, APP 7 is particularly difficult and complex. The committee has concerns that this will adversely affect the implementation of this principle and for this reason believes that further consideration be given to the structure and language used in the principle.

Recommendation 10

10.46 The committee recommends that the drafting of APP 7 be reconsidered with the aim of improving structure and clarity to ensure that the intent of the principle is not undermined.

Defining 'direct marketing'

10.47 Some submitters noted that a definition of 'direct marketing' has not been provided in the exposure draft.[52] The ABA noted that, due to the reference in APP 7(6) to the SPAM and DNCR Acts, the absence of a specific definition allows the interpretation that direct marketing as used in the principle, 'is confined to direct marketing by means other than the means covered under those Acts'.[53]

10.48 Privacy Law Consulting Australia noted that as two differing definitions of the term 'direct marketing' are provided in the Australian Direct Marketing Association's *Direct Marketing Code of Practice* (2001) and the OPC's *Draft NPP*

---

50 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 905; Australian Government, *Enhancing National Privacy Protection*, p. 57.

51 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 893–898; Australian Government, *Enhancing National Privacy Protection*, p. 56.

52 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 1; Australian Bankers' Association, *Submission 15*, p. 8; Privacy Law Consulting Australia, *Submission 24*, pp 4–5.

53 Australian Bankers' Association, *Submission 15*, p. 8.

Guidelines (7 May 2001), it would be useful to have the term defined in the new Privacy Act, particularly as the definition of this term will determine the activities to which APP 7 applies.[54]

10.49 The ALRC report noted calls from stakeholders for a definition of direct marketing to be provided in the Privacy Act, however, the submissions received did not provide consensus on how the term should be defined. Further, the ALRC expressed concern that providing a definition of direct marketing 'may unnecessarily confine the application of the 'Direct Marketing' principle'. Therefore the ALRC considered that direct marketing should not be defined in the Privacy Act.[55]

10.50 The committee notes the department's response that there is no intention to include a definition of 'direct marketing' in the Act and that the current Act does not define direct marketing. Further, the Government accepted the ALRC's view as outlined above.

Application to agencies

10.51 APP 7 applies to organisations and those agencies which engage in commercial activities, as provided by existing section 7A of the Privacy Act. This was supported by some submitters, including Privacy Victoria.[56] However, other submitters argued that, as a number of agencies, both at the Commonwealth and State and Territory level, engage in direct marketing, APP 7 should apply to all entities.[57] Professor Graham Greenleaf and Mr Nigel Waters stated:

> We believe the principle should apply to both agencies and organisations on the grounds that the boundaries between private and public sectors are increasingly blurred, and government agencies are now commonly undertaking direct marketing activities.[58]

10.52 Professor Greenleaf and Mr Waters noted that while under section 7A of the current Privacy Act, APP 7 would apply to the commercial activities of some prescribed agencies, this is not sufficient, particularly as the exemption for the majority of agencies has been extended under APP 7(1)(c).[59]

---

54 Privacy Law Consulting Australia, *Submission 24*, pp 4–5.

55 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 896–898.

56 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 7.

57 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 11; Australian Direct Marketing Association, *Submission 27*, pp 7-8.

58 Professor G Greenleaf & Mr N Waters, *Submission to the Australian Law Reform Commission on the Review of Australian Privacy Law Discussion Paper 72: Strengthening uniform privacy principles: an analysis of the ALRC's proposed principles*, 17 December 2007, pp 44–45; See also Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 11.

59 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 11.

10.53 In addition, concern was expressed by the ADMA that as currently drafted, APP 7 may have the effect of requiring agencies to discontinue their direct marketing activities, or be forced to justify their direct marketing activities under APP 6, which does not afford the same level of privacy protection regarding direct marketing as APP 7.[60]

10.54 In light of these issues, some submitters recommended that references to 'organisation' in APP 7 should be changed to 'entity'. Professor Greenleaf and Mr Waters submitted that if this change were made, an additional provision providing an exception regarding information for the purpose of direct marketing communications which are required or authorised by law would need to be inserted.[61]

10.55 The OPC commented that it is not clear whether the note to APP 7(1) is intended to give force to the position in the Government's response, which suggested that agencies which engage in commercial activities should be 'required to comply' with the APPs. It was noted that this position differed from the ALRC recommendation, which suggested that the direct marketing principle should only apply to organisations, and agencies should comply with the direct marketing principle as a matter of 'best practice'.[62]

10.56 The ALRC provided commentary on the basis of its recommendation concerning direct marketing in relation to agencies. Mr Bruce Alston, Senior Legal Officer at the ALRC, stated that:

> When looking at whether it should include agencies—that is, Commonwealth government agencies—we obviously rejected that idea and instead went for organisations with an extension to contracted service providers, in the same way a lot of other Commonwealth laws reach out and cover people providing services to the Commonwealth as well as to agencies.[63]

10.57 Professor Rosalind Croucher, President of the ALRC further elucidated:

> There is a distinction made between organisations and entities but I think the overall approach is that similar principles should apply. There is a distinction between public and private sector. It necessarily is that way, and that is partly because of the constitutional backdrop. The idea is that there should be similar obligations with respect to all.[64]

---

60 Australian Direct Marketing Association, *Submission 27*, pp 7–8.

61 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 11; Australian Direct Marketing Association, *Submission 27*, pp 7–8.

62 Office of the Privacy Commissioner, *Submission 39*, p. 36.

63 Mr Bruce Alston, Senior Legal Officer, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 8.

64 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 8.

Conclusion

10.58 The committee notes that the ALRC considered arguments for the extension of the application of direct marketing requirements to agencies. However, the ALRC formed the view that if direct marketing requirements were extended to apply to agencies, the way that government agencies communicate with individuals would be significantly affected. The Government agreed that the application of direct marketing requirements to agencies would not be appropriate.[65] Further, in its submission to the ALRC review, and in its submission to this inquiry, the OPC noted that the use and disclosure of personal information by agencies would still be regulated, as agencies will be required to abide by the use and disclosure principle in their management of personal information.[66]

10.59 The committee concurs with the Government's view that the direct marketing principle should only apply to agencies in specific circumstances. However, mindful of the OPC's comments, the committee considers that the draft note to APP 7(1) should be redrafted to better reflect the Government's position.

Recommendation 11

10.60 The committee recommends that the note to APP 7(1) be redrafted to better reflect the position outlined in the Government response.

Direct marketing to minors

10.61 Some submitters expressed concern that the exposure draft does not expressly prohibit direct marketing to minors. The Public Interest Advocacy Centre (PIAC) noted that where UPP 6 contained a reference to children under the age of 15 years, APP 7 makes no mention of minors. PIAC argued that direct marketing to children under 15 years of ages should be prohibited, with the possible exception of existing customers and targeted public health and safety campaigns. Although PIAC acknowledged that ascertaining the age of an individual can be difficult, it noted that if an organisation has sufficient personal information to undertake direct marketing, it should be able to ascertain the individual's age, and obtain their consent before undertaking direct marketing.[67]

10.62 The Obesity Policy Coalition expressed similar concerns, and recommended that APP 7 be amended to prevent an organisation from using or disclosing personal

65 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 899–903; Australian Government, *Enhancing National Privacy Protection*, p. 56.

66 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 899–903; Office of the Privacy Commissioner, *Submission 39*, p. 36.

67 Public Interest Advocacy Centre, *Submission 32*, p. 1; *Attachment 1*, p. 11; Obesity Policy Coalition, *Submission 40*, pp 2–3.

information of an individual who is known to be, or is reasonably likely to be, younger than 15 years old, for the purposes of direct marketing, unless express and verifiable consent has been provided by a parent, or the organisation can confirm that the individual is older than 15 years of age. The Obesity Policy Coalition suggested this is particularly important as most young children under 15 years of age do not have the capacity to make informed decisions about the use of their personal information, and are more susceptible to commercial influence.[68]

10.63 The Government response acknowledged concerns raised in the ALRC's review about the potential impact of direct marketing on individuals under 15 years of age, in particular direct marketing via email and SMS. However, the Government was 'not convinced that there is sufficient justification for distinguishing direct marketing obligations on the basis of an individual's age'. The Government formed this view on the basis that:

- in effect, the Privacy Act chiefly relates to postal direct marketing and there is insufficient evidence that this form of marketing has adversely affected young people; and
- if organisations are required to establish an individual's age, they may collect more information about the individual than would otherwise be necessary.[69]

10.64 Consequently, the Government concluded that applying different standards for the use and disclosure of personal information for the purpose of direct marketing on the basis of an individual's age would only increase the burden on organisations, and the complexity of the principles, without providing commensurate benefit. However, the Government did encourage the OPC to issue guidance on the obligations of organisations regarding direct marketing to vulnerable people, should the Privacy Commissioner decide it is appropriate to do so.[70]

Conclusion

10.65 While acknowledging the concerns of commentators about the impact of direct marketing to minors, the committee is mindful that the Privacy Act will primarily regulate direct marketing via post and that there is insufficient evidence that postal direct marketing to young people has resulted in substantial adverse consequences. Therefore, the committee does not consider that specific prohibition of direct marketing to minors is required in the Privacy Act but is of the view guidance from the Australian Information Commissioner on direct marketing to vulnerable people, as suggested by the Government, would be beneficial.

68 Obesity Policy Coalition, *Submission 40*, pp 2–3.

69 Australian Government, *Enhancing National Privacy Protection*, pp 57–58.

70 Australian Government, *Enhancing National Privacy Protection*, pp 57–58 and 60.

Recommendation 12

10.66 The committee recommends that the Australian Information Commissioner develop guidance in relation to direct marketing to vulnerable people.

'Existing' and 'non-existing' customers concept

10.67 The Companion Guide explains that while the terminology used in APP 7 is different to that in the Government response: rather than 'existing' and 'non-existing' customers, APP 7 focuses on individuals who have provided personal information to the entity which is undertaking the direct marketing (APP 7(2) and people who have not provided information (APP 7(3)).[71] The Companion Guide states that the same policy is achieved and that the policy intent is to apply more stringent obligations when using personal information of non-existing customers as the individual is less likely to expect use or disclosure for direct marketing purposes.

10.68 The department noted that:

> In the case of personal information that is not sensitive information the requirements that are stated in the Government response to apply to 'existing customers' will apply where the information was collected from the individual. Further, they apply where the individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing.
>
> The requirements that apply to 'non-existing customers' in the Government response will apply where the information was not collected from the individual (or, for logical consistency, where the 'existing customer' would not have reasonably expected that the organisation would use or disclose the information for the purpose of direct marketing).[72]

10.69 Submitters raised a range of concerns including the difficulties of the implementation of the principle. Australian Direct Marketing Association (ADMA), for example, submitted that this approach is 'unworkable' as industry process cannot be neatly divided into two streams on the basis of whether the information was obtained from the individual or not. Further, ADMA argued that it would be very difficult, even for external agencies such as regulators, to independently assess whether APP 7(2) or APP 7(3) applies in any given situation. ADMA stated that it rejected the approach taken by the Government and submitted that the principles should revert to the structure as recommended by the ALRC.[73] ADMA also argued that there would be significant additional complexity for organisations as they would be required to examine on a case-by-case basis, each campaign and potentially each

71 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 11.

72 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 18.

73 Australian Direct Marketing Association, *Submission 27*, pp 4–5.

individual record to determine whether any elements of the information that is being used or disclosed was not obtained from the individual.[74]

10.70 ADMA concluded:

> The move to information source represents a significant departure both from the stated policy that different regimes would apply depending on whether an organisation has an existing relationship with the individual, but more importantly does not satisfactorily meet the criteria set by the Government of introducing a simpler regime.[75]

10.71 The OPC noted that APP 7 appears to be more complex than outlined in the Companion Guide as there are exceptions which depend on individuals' reasonable expectations for use and disclosure. The OPC suggested that 'the language in the principle could more clearly distinguish between individuals who have an established relationship with an organisation and those who do not'.[76]

10.72 The OPC commented further that the Spam Act, the DNCR Act and ADMA Direct Marking Code of Practice use the concept of 'on-going' or 'pre-existing' relationships for direct marketing. The OPC suggested that there would be advantage to adopting terms from those Acts or codes as this would ensure that:

- APP obligations are well understood across the industry and smoothly incorporated within existing compliance frameworks; and
- individuals can readily understand their rights, and marketers' obligations.

10.73 ADMA and The Communications Council also supported the alignment of the Privacy Act with the SPAM and DNCR Acts.[77] ADMA noted that 'existing relationship' is widely understood by industry and that it would provide a consistent approach with other privacy related laws.[78]

10.74 The Communications Council was concerned that the provisions of APP 7(3) may apply in the case where an entity may use information gained from existing customers to make inferences on customer interest in purchasing products or services. This would result in more 'onerous requirements to provide opt-out facilities and opt-out statements'. Further, 'this would have an adverse effect on direct marketing and jeopardises marketing agencies' existing relationships with individuals'.[79]

---

74 Australian Direct Marketing Association, *Submission 27*, p. 6.

75 Australian Direct Marketing Association, *Submission 27*, p. 6.

76 Office of the Privacy Commissioner, *Submission 39*, p. 34.

77 Australian Association of National Advertisers, *Submission 21*, p. 7.

78 Australian Direct Marketing Association, *Submission 27*, pp 4–5.

79 The Communications Council, *Submission 23*, p. 8.

10.75 The ABA noted that the 'existing' and 'non-existing' distinction is helpful for compliance. However, the ABA argued that the provisions of APP 7(3) meant that this distinction between customers is lost:

> The distinction between existing and non-existing customers becomes confused by the provisions of APP 7 (3)(a)(i) that suggest that the personal information, although collected from an existing customer by the organisation, must be handled differently because that individual would not reasonably expect the information to be used by the organisation for direct marketing. The advantage of the distinction between existing and non-existing customers is therefore significantly lost.[80]

10.76 The OPC also suggested that the Government's concerns about the use of the term 'customer' could be overcome by the inclusion of a definition or by the concept of ongoing or existing relationships.[81]

10.77 The department provided the committee with comments on the issues raised in submissions and stated that:

> The drafting approach taken does not divert from the Government's response. The focus in APP 7 is on the key elements of an existing customer relationship, and this is different to the more ambiguous and potentially broader 'existing relationship' concept in the Spam Act 2003 and the Do Not Call Register Act 2006. The approach of distinguishing a customer from a non-existing customer by whether information is provided is the best drafting approach to defining an 'existing customer'. The consequence may be that the requirements in the Privacy Act may differ from sectoral specific legislation but that is necessary to ensure that concepts in the Privacy Act (particularly relating to consent) are consistent and unambiguous.[82]

10.78 The department went on to state that the 'existing relationship' concept in the Spam Act and the Do Not Call Register Act is appropriate for the sectoral specific direct marketing practices relating to electronic messages and phone calls. That concept is included within a broader notion of 'inferred consent', which is based on consent that 'can be reasonably inferred from the conduct, and the business and other relationships, of the individual or organisation concerned'.[83]

Conclusion

10.79 The committee notes that many submitters raised significant concerns with the concepts in APP 7. However, the Companion Guide and the department's answer make clear that the policy outlined in the Government response is achieved. Further,

---

80 Australian Bankers' Association, *Submission 15*, p. 8.

81 Office of the Privacy Commissioner, *Submission 39*, pp 34–35.

82 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 18.

83 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 19.

the 'existing relationship' concept in the Spam Act and the Do Not Call Register Act is more ambiguous and potentially broader. The committee therefore does not consider that any amendment to this concept is required.

10.80 In relation to the simplification of the principle, the committee considers that further consideration be given to the inclusion in APP 7(3) of the provision in relation to the use and disclosure of information collected from an individual when the individual would not have reasonably expected the information to used or disclosed for the purpose (APP 7(3)(a)(i)). This adds to the difficulties of interpreting the principle.

Recommendation 13

10.81 The committee recommends that the structure of APP 7(2) and APP 7(3) in relation to APP 7(3)(a)(i) be reconsidered.

Personal information collected from the individual–APP 7(2)

10.82 APP 7(2) provides that information collected from the individual can be used or disclosed for direct marketing purposes if the individual would 'reasonably expect' the organisation to undertake that activity, the organisation provides a simple means for the individual to not request not to receive the direct marketing communications; and the individual has not requested that information be not received.

10.83 Issues raised in relation to this provision included the need for clarification of terms and guidance.

10.84 The ABA commented that wording of APP 7(2)(a) in relation to aggregation products and noted that these products typically involve an agreement with the customer to source and aggregate financial information about the customer from the customer's other financial institutions using the customer's credentials. Information acquired this way is compiled into financial statements and can be made available to the customer in a useful format in secure internet banking sessions. Informed consent for the collection underpins the arrangement. As part of the terms of these products the bank may use this information for marketing purposes. The ABA commented the wording of APP 7(2) would require excessive disclosure of the customer's right to opt out in these circumstances.[84]

10.85 Submitters requested guidance as to what would constitute a 'simple means' for an individual to request not to receive direct marketing information. Epworth HealthCare suggested that it may be useful if examples are provided.[85] The Law Institute of Victoria (LIV also identified this issue, and suggested that an amendment be made to indicate that in relation to electronic communications, 'simple means' is

84 Australian Bankers' Association, *Submission 15*, p. 9.

85 Epworth HealthCare, *Submission 9*, p. 1.

subject to additional obligations under the Spam Act.[86] Submitters also suggested that guidance would be as to the types of direct marketing communications for which an individual might 'reasonably expect' an organisation to use or disclose their personal information, and the circumstances in which it might be impracticable for an organisation to seek an individual's consent to use or disclose their information for the purposes of direct marketing.[87]

10.86 Professor Greenleaf and Mr Waters raised concern that use of the phrase 'collected the information from the individual' in APP 7(2)(a), instead of the expression 'provided by', might lead to an interpretation that 'reasonable expectation' under APP 7(2)(b) would also apply to non-consensual collection of information. It was argued that:

> For the principle to achieve its objective, it is essential that the lesser protection afforded to 'existing customers' should only apply where the individual has knowingly and voluntarily provided the information. It would not be acceptable for individuals be denied an 'opt-out' either because their information had been collected without their knowledge (as is often the case in internet use) or because they had been required (e.g. by law) to provide it (as is the case with many financial, telecommunications and government transactions under statutory 'customer identification' requirements).[88]

10.87 The National Australia Bank (NAB) noted concern that APP 7 does not adequately cover circumstances in which an organisation collects personal information from an individual for the primary purpose of direct marketing, as it requires a test under APP7 (2)(b) as to whether 'the individual would reasonably expect the organisation to use or disclose the information for that purpose'. The NAB suggested that this is inconsistent with APP 6 which states that if an entity has collected information for a particular purpose (the primary purpose), it may use and disclose the information for that purpose without further assessment.[89]

10.88 The Australian Finance Conference (AFC) noted that no specific consent provision regarding the use or disclosure of information collected without the individual's consent has been provided in APP 7(2). The AFC suggested that even though APP 7(2)(b) provides a general permission, a specific provision regarding consent to the use or disclosure of information collected without the individual's consent would assist compliance certainty.[90]

---

86 Law Institute of Victoria, *Submission 36*, pp 6–7.

87 Financial Services Council, *Submission 34*, pp 2–3.

88 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 12.

89 National Australia Bank, *Submission 2*, p. 4.

90 Australian Finance Conference, *Submission 12*, pp 6–7.

Conclusion

10.89 The committee considers that guidance on the provisions of APP 7(2) and APP 7(3) would be useful.

Personal information collect from another person–APP 7(3)

10.90 As noted above, APP 7 provides for more stringent obligations in relation to the use or disclosure of information collected from another person. The AFC noted that the drafting of this provision required some clarification, and suggested it be redrafted, as it is unclear 'how an individual would not reasonably expect the organisation to use/disclose personal information for direct marketing [APP 7(3)(a)(i)] if the individual had consented to the use/disclosure [APP 7(3)(b)(i)].'[91]

Consent

10.91 Telstra Corporation Limited (Telstra), noted that the requirement in APP 7(3) for an organisation to obtain an individual's consent before using or disclosing personal information about them received from a third party, appears quite broad. Concern was raised that this requirement may oblige an organisation to obtain consent to use publicly available information or updated information provided by an authorised representative on a customer's account. Telstra suggested that to address this issues, the phrase 'would not reasonably expect' be included at the end of APP 7(3)(a)(ii), and that information obtained from authorised representatives and third parties working for or affiliated with the organisation be excluded from requirements under the provision.[92]

Opt-out provisions–APP 7(1)(a),(2)(c),(3)(c)(d) and (4)

10.92 A number of comments were made about the 'opt-out' provisions under APP 7. The OPC suggested that the opt-out requirements in the principle could be simplified by consolidating APP 7(4) and APP 7(5) and modelling it more closely on UPP 6.3.[93]

10.93 Professor Greenleaf and Mr Waters commented on the difference in the provisions of APP 7(2) and (3). They stated that APP 7(2) does not require the opt-out to draw an individual's attention to the provision although this is included in APP 7(3). They commented:

> Under (2), if the individual would reasonably expect to receive marketing communications, they are not even required to be notified – this seems perverse and is a very weak provision. All the evidence suggests that most individuals are only too aware that they are likely to receive direct

91 Australian Finance Conference, *Submission 12*, p. 7.

92 Telstra Corporation Limited, *Submission 19*, p. 3.

93 Office of the Privacy Commissioner, *Submission 39*, pp 35–36.

> marketing from organisations with which they have dealt, but that it is precisely these communications they wish to be able to stop![94]

10.94 Concerns were also raised that the opt-out provision is weak and can be circumvented. Privacy Law Consulting Australia noted that APP 7(4)(b) refers to 'direct marketing by other organisations' therefore, if an organisation markets on behalf of persons or bodies which are not organisations as defined by the Act, they will not be required to comply with the provision.[95]

10.95 Submitters also commented about the lack of a provision to require organisations to provide individuals with the option to opt-out of the provision of sensitive information for direct marketing purposes.[96] Privacy Law Consulting Australia stated that this is most likely because consent is required in all circumstances for the use of this information for direct marketing, and that such consent can be revoked at any time. However, it was submitted that the requirement that sensitive information only be disclosed or used with consent is undermined by the definition of 'consent' in the Act, which includes 'implied consent'. It was suggested that express consent should be required regarding the disclosure and use of sensitive information, and that consideration be given to whether an opt-out facility should be required in relation to the use of sensitive information for direct marketing purposes, to facilitate individuals exercising their right to withdraw consent.[97]

10.96 The department responded that under APP 7(1)(a), sensitive information about an individual can only be used for direct marketing by an organisation with the consent of that individual unless the organisation is a contracted service provider for a Commonwealth contract and the organisation collected the information for the purpose of meeting an obligation under the contract. The concerns expressed are that, at some point in the future, the individual may want to revoke consent or opt-out (i.e. no longer wants to receive direct marketing communications from the organisation). Further:

> There would be options available to individuals in this instance. First, as noted by the PLCA, consent could be revoked at any time, in which case the organisation could not use sensitive information for direct marketing purposes.
>
> While it is a matter for the [Australian Information Commissioner], guidelines to be prepared on the meaning of 'consent' are likely to address key issues such as revocation.
>
> In addition, as a result of APP 7(2) and (3), organisations will be required in practice to provide a simple means by which an individual may easily

94 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 12.

95 Privacy Law Consulting Australia, *Submission 24*, p. 5.

96 Financial Services Council, *Submission 34*, p. 2.

97 Privacy Law Consulting Australia, *Submission 24*, p. 5; Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 12–13; Financial Services Council, *Submission 34*, pp 2–3.

> request not to receive direct marketing communications from an organisation. Further, APP 7(4)(a) provides that an individual may request not to receive direct marketing communications from the organisation.[98]

10.97 The department also stated that:

> Obtaining consent and including opt-out facilities should be encouraged as part of a direct marketing organisation's internal procedures. As with other new APPs, there is scope for the AIC to provide guidance on the operation of these provisions. If guidance on the practical workings of APP 7 became necessary, the Department will liaise with the AIC to consider whether to develop guidelines.[99]

10.98 Some submitters argued that the APP imposes an excessive requirement to disclose customers' right to opt-out, and the ABA recommended particular changes to APP 7(2) and (3) in its submission to address these concerns.[100] The ABA and other submitters also suggested that APP 7(4) should allow for an option not to receive any direct marketing at all or that organisations should only have to provide opt-out information to non-existing customers.[101]

10.99 APP 7(3)(d) provides that in each direct marketing communication with the individual, a prominent must be included that the individual can make a request to opt out or draws attention of the individual to this option by another means. Telstra argued that this provision would not be required for customers who had already received the entity's privacy statement that has set out this information and should only apply where the individual has not already received the entity's privacy statement.[102]

10.100 ADMA raised similar concerns about the obligations on organisations and facilitating organisations under APP 4, noting that in its understanding:

> ...the organisations whose products and services are being advertised (the marketing organisation) will carry the responsibility for receiving and actioning a request by the individual not to have their data used in the future for direct marketing purposes. In such circumstances the marketing organisation may put in place processes for its suppliers (facilitating organisations) to accept and forward on those opt out requests however the facilitating organisations would not in this circumstance be required to not contact the individual again on behalf of other marketing organisations.[103]

---

98 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, pp 21–22.

99 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 21.

100 Australian Bankers' Association, *Submission 15*, pp 9-10; Telstra Corporation Limited, *submission 19*, p. 3; Communications Council, *Submission 23*, p. 7.

101 Australian Bankers' Association, *Submission 15*, p. 9; Telstra Corporation Limited, S*ubmission 19*, p. 3.

102 Telstra Corporation Limited, *Submission 19*, p. 3.

103 Australian Direct Marketing Association, *Submission 27*, pp 6–7.

10.101 Given this apparent uncertainty, ADMA suggested that the exposure draft should specify that facilitating organisations, which do not provide direct marketing communications in their own right, will be exempt from APP 7(3)(c), and:

> ...will not be bound by the Act to not contact the individual again where a subsequent direct marketing communication is originated by the facilitating organisation on behalf of another marketing organisation that is wholly unrelated to the original marketing organisation that the individual's opt out request was directed.[104]

Conclusion

10.102 The committee notes that the ALRC review suggested that the opt-out notification obligations should differ for existing and non-existing customers.[105] While the exposure draft has taken a different approach, it has still provided a distinction in the required level of notification regarding the ability of an individual to opt-out. In circumstances in which the information has been collected from the individual, an organisation merely has to provide a simple means by which an individual can opt-out of receiving future direct marketing communications. Where the information about an individual has been collected from a third party, in each direct marketing communication, the organisation must notify the individual of their ability to opt-out of receiving future direct marketing communications from the organisation.

10.103 Further to its comments in chapter 3, the committee considers that further guidance on the definition of consent will assist in the interpretation of the principle.

Source of information–APP 7(4)(c) and (5)

10.104 APP 7(4)(c) provides for an individual to request the organisation to provide the source from which they obtained personal information about the individual. APP 7(5)(c) provides that an organisation must notify the individual or the sources within a reasonable period 'unless it is impracticable or unreasonable to do so'. Professor Greenleaf and Mr Waters expressed concern that the exception in APP 5(c) 'unless it is impracticable or unreasonable to do so' is too broad, and consequently is likely to be misused, thereby undermining the purpose of the principle.[106]

10.105 However, a number of submitters argued that the provisions of APP 7(4)(c) are onerous and impractical.[107] For example, Coles commented on the wide range of

---

104 Australian Direct Marketing Association, *Submission 27*, pp 6–7.

105 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 915.

106 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

107 The Westpac Group, *Submission 13*, p. 2; Australian Bankers' Association, *Submission 15*, p. 9; Insurance Council of Australia, *Submission 17*, p. 2; Communications Council, *Submission 23*, p. 7; Privacy Law Consulting Australia, *Submission 24*, pp 6–7.

sources used to collect personal information including emails, in-store transactions and competitions. Once information is collected via some sources, it is no longer possible to determine the source of the information, and changing IT systems for this purpose is likely to be impractical and prohibitively expensive. Coles noted the exception provided for in APP 7(5), however, remained concerned that:

> ...this exemption is as yet unclear as to whether not keeping track of such information will be sufficient for reliance on an ongoing basis or whether an organisation will be required in future to change its systems or selection of its systems to ensure compliance with APP(4) going forward. This is likely to impose a significant administrative and costs burden on organisations.[108]

10.106 Coles went on to comment that the exemption in APP 7(5) could be amended to provide a further exemption that identification of the source of the personal information will not be required if the specific source of the information is not traceable, provided that the organisation can identify the possible or likely sources of collection.[109]

10.107 Coles' concerns were echoed by the Westpac Group, which noted that this requirement could not be retrospectively applied. Consequently, the Westpac Group indicated its support for the Australian Bankers' Association suggestion that the requirement to record the source of information received from third parties for the purposes of direct marketing, and the requirement to inform those third parties of any change to the information held by an organisation, should be limited to non-existing customers.[110]

10.108 Further guidance and clarification on these provisions was sought by the Financial Services Council (FSC), which suggested that the principle should explicitly state that organisations are not required to disclose the ultimate source of information, only the source from which the organisation obtained the information. The FSC also suggested further guidance regarding the factors an organisation should consider in determining whether it is reasonable and practical to advise an individual of the source from which it obtained the individual's information.[111]

10.109 Privacy Law Consulting Australia noted uncertainty regarding the construction of APP 7(5)(c), as it appears unclear whether 'impracticable or unreasonable' applies to the 'reasonable period' or the notification of the individual. It was suggested that this be clarified in the legislation.[112]

---

108 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 2.

109 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 2.

110 The Westpac Group, *Submission 13*, p. 2; Australian Bankers' Association, *Submission 15*, pp 10–11.

111 Financial Services Council, *Submission 34*, pp 2–3.

112 Privacy Law Consulting Australia, *Submission 24*, pp 6–7.

10.110 The department responded to these concerns and stated that this language is consistent with the ALRC recommendation that source disclosure be mandated upon request 'where reasonable and practicable'. The ALRC review noted that an obligation to advise individuals, in response to a request, of the source from which their personal information was obtained might increase the compliance burden on organisations. In light of this the ALRC suggested that the obligation should only apply where 'reasonable and practicable', and should be limited to individuals who are non-existing customers.[113] The department provided the example of information that was recorded at a time where an organisation has not been required to record, and not recorded, the source of this information, then it would be unreasonable to expect an organisation to provide this information.

10.111 The department went on to stated that:

> While some organisations may attempt to misuse this test, it is a necessary element of the legislation to enable the policy goal of source disclosure to existing customers who have not provided information to organisations. It is also possible to clarify this issue in the Explanatory Memorandum when the Privacy Act is considered by the Parliament.[114]

10.112 The ALRC also formed the view that the organisation should only be required to name the direct source from which the organisation obtained the individual's information, rather than the original source of information.[115]

Interaction with other legislation–APP 7(6)

10.113 APP 7(6) provides that the principle does not apply to the extent that any of the DNCR Act, the Spam Act or any other Act prescribed by the regulations apply. Comments in relation to APP 7(6) went to the effect of this provision and the need for clarity.[116] Some submitters suggested that the inclusion of this section means that in effect, the Privacy Act will only apply to marketing activities via direct mail and this could result in confusion about handling personal information. Coles commented:

> APP 7(6) suggests that an organisation will not be required to deal with personal information in accordance with APP 7 for direct marketing activities like emails, faxes and telephone contact provided that the activities are done with the individuals consent as these activities are otherwise dealt with under the Spam Act 2003 or the Do Not Call Register Act 2006. As each regime requires a different approach to the handling and use of personal information, this is likely to increase the likelihood of

113 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 925–26.

114 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 23.

115 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 925–26.

116 See for example, Australian Institute of Credit Management, *Submission 8*, p. 3; Abacus Australian Mutuals, *Submission 7*, p. 2.

> confusion arising and the incorrect regime being applied to the handling and use of the information.[117]

10.114 Privacy Law Consulting Australia expressed uncertainty as to the meaning of the phrase 'apply to the extent that' as the Spam or DNCR Acts regulate activities, not the handling of personal information per se. Consequently:

> It appears that the intention is that, if one of the Acts permits an activity that necessarily involves the use or disclosure of personal information in a particular manner, APP 7 does not apply to such use or disclosure. For example, the Spam Act permits commercial emails to be sent with consent. This suggests that an organisation will be permitted to use or disclose personal information to send such emails in accordance with the Spam Act, regardless of requirements that might otherwise apply under APP 7.[118]

10.115 Coles suggested that this confusion could be addressed by incorporating the obligations under the Spam and DNCR Acts into the new exposure draft, thereby reducing the complexity of the legislation, and ensuring that the obligations of organisations and the protections for individuals are unambiguous and clearly set out in one document. Coles went on to suggest that the obligations of the Spam and DNCR Acts would be incorporated in the Privacy Act as 'this would reduce the complexity of the law in this area and reduce the likelihood of unintentional inappropriate use of personal information in the area of direct marketing activities.[119]

10.116 Although APP 7(6)(c) refers to 'any other Act', the AFC suggested that the interaction between APP 7 and the anti-hawking provisions in the *Corporations Act 2001*, requires clarification, it may increase compliance certainty if those anti-hawking provisions are specifically included in the list under APP 7(6).[120]

10.117 The department provided a response to this comment and stated that the Government agreed with the ALRC's recommendation that the 'direct marketing' principle should be displaced to the extent that more specific sectoral legislation regulated a particular type of direct marketing or direct marketing by a particular technology. Further, that the ALRC believed this approach was preferable because imposing a blanket rule for all forms of direct marketing was too rigid. It stated that other forms of more intrusive direct marketing should be subject to regulation that differs from the rules applicable to less intrusive forms of direct marketing. It noted that, relying on such sectoral legislation to the exclusion of the Privacy Act is problematic, because it leaves loopholes that could encourage other types of direct marketing that also may be intrusive.

---

117 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 2; see also Australian Institute of Credit Management, *Submission 8*, p. 3.

118 Privacy Law Consulting Australia, *Submission 24*, pp 7–8.

119 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 2.

120 Australian Finance Conference, *Submission 12*, p. 7.

10.118 The department concluded that 'this is reflected in APP 7(6) which provides that APP 7 does not apply to the extent that the Spam Act, the Do Not Call Register Act, or any other Act of the Commonwealth prescribed by the regulations applies'. Further 'this means that APP 7 will apply to organisations involved in direct marketing relating to electronic messages and phone calls, where acts and practices are not covered by those Acts'.[121]

121 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 20.

Chapter 11

Australian Privacy Principle 8–cross-border disclosure of personal information and sections 19 and 20

Introduction

11.1 Australian Privacy Principle 8 (APP 8) outlines measures to ensure that entities cannot avoid obligations to protect personal information by disclosing the information to a recipient outside Australia.[1] Section 19 provides for the extra-territorial operation of the new Privacy Act.[2] Section 20 provides that an entity remains accountable for the acts and practices of overseas recipients to which it discloses personal information.[3]

11.2 The Companion Guide notes that APP 8 uses the term 'disclosure', rather than 'transfer', which was used in National Privacy Principle 9 (NPP 9) as 'transfer' implies that there is a cross-border movement of personal information rather than the accessing of personal information by an overseas recipient, regardless of whether the information is stored in Australia or elsewhere through 'disclosure'. The Companion Guide notes that the routing of personal information through servers which are located outside of Australia is not intended to constitute a disclosure.[4]

11.3 APP 8 has been extended to apply to agencies as well as organisations.[5] In addition, APP 8 provides conditions for the disclosure of personal information outside Australia to ensure that entities remain accountable for any disclosures they make, rather than prohibiting cross-border disclosures all together as is the case under NPP 9. However, a series of exceptions provide for an entity not to be held accountable for the disclosure of personal information to an overseas recipient.[6]

11.4 The principle provides that before disclosing any personal information outside of Australia, an entity has to take 'reasonable steps' to ensure that the overseas recipient will not breach the APPs, by making sure that personal information has sufficient protection. The Companion Guide notes it is expected that the obligations of the overseas recipient would be set out in a contract to establish effective information management arrangements.[7]

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

2 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 6–7.

3 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

4 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

5 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

6 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

7 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

11.5 Section 19 provides for the extraterritorial operation of the Act. In addition, unlike the *Privacy Act 1988* (Privacy Act) which only extended to the acts or practices undertaken by an organisation outside of Australia in relation to the personal information of Australian citizens or permanent residents, the new Privacy Act will extend to protect every person, operating in relation to acts done or practices engaged in outside of Australia, by agencies and organisations with an Australian link.[8] The definition of an 'Australian link' is similar to that provided under subsection 5B(2) of the current Privacy Act.[9]

11.6 The Companion Guide also states that arrangements under the existing Privacy Act which ensure that an act or practice that is done or engaged in outside Australia is not an interference with privacy if the act or practice is required by an applicable law of a foreign country, will be replicated in the new Privacy Act. These provisions will extend to cover agencies as well as organisations.[10]

11.7 Under proposed section 20, an entity is held accountable for the acts and practices of overseas recipients.[11] The Companion Guide notes that while the term 'accountability' is not used in this section, the provisions of the section hold an entity as liable for the acts and practices of an overseas recipient which breach the APPs. However, if one of the exceptions under APP 8 applies to the entity, then section 20 will not apply to the entity.[12]

Background

11.8 The transfer of personal information across national borders has been identified as an issue of significant community concern. However, technological advancements, among other developments, have contributed to a change in the way business is conducted, and how personal information is collected and managed.[13] A submitter to the Australian Law Reform Commission (ALRC) review commented:

> In today's truly globalised world, cross-border data flows are an everyday fact of commercial public and private life. The challenge therefore becomes how to maintain a consistent security and privacy framework around the treatment of that information across legal and jurisdictional borders and geographies.[14]

---

8 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 6–7.

9 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 20.

10 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 7.

11 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

12 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

13 Microsoft, *Submission 14*, p. 5; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1063–65.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1065.

11.9 International frameworks for privacy protection have also been developed in response to the global developments 'to harmonise laws within economic communities and improve trade relationships.' These include the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines); European Union (EU) *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive); and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[15]

11.10 Currently, NPP 9 provides the specific circumstances in which an organisation can transfer information to a recipient in a foreign country, and is largely modelled on articles 25 and 26 of the EU Directive. There are no requisite arrangements in the Information Privacy Principles (IPPs) which apply to agencies.[16]

11.11 Notably, NPP 9 does not apply where the information is transferred to the same organisation, rather it only applies if the transfer is to a third party. Further, NPP 9 only regulates the transfer of information to 'foreign countries' as opposed to 'other jurisdictions', and therefore:

> It does not protect personal information that is transferred to a state or territory government that is not subject to privacy law, or a private sector organisation that is exempt from the Privacy Act.[17]

11.12 Section 5B of the current Privacy Act ensures that organisations do not avoid their obligations in relation to the management of personal information under the Act by transferring information overseas. The Privacy Act applies to an act or practice relating to personal information about an Australian citizen or permanent resident, and the organisation undertaking the act or practice either has an Australian link or carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.[18] To implement this, Privacy Commissioner's enforcement powers are extended to overseas complaints which fit specified criteria.[19]

11.13 Subsection 6A(4) and section 13D of the existing Privacy Act provide that an act or practice undertaken overseas which is required by an applicable foreign law will

---

15 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1065–66.

16 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1086–87.

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1086–87.

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1081–82.

19 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1082.

generally not be taken as a breach of the Act or an interference with the privacy of an individual.[20]

11.14 The ALRC review looked at the following matters, among others:

- international frameworks for privacy protection, in particular, the EU Directive, the APEC Privacy Framework and the Asia-Pacific Privacy Charter;
- regulation of cross-border data flows under the *Privacy Act 1988* via the extraterritorial operation of the Act;
- the restrictions in NPP 9 on the transfer of personal information to countries with differing privacy regimes;
- the content of the 'Cross-border Data Flows' principle in the model Unified Privacy Principles (UPPs) and its application to agencies and related bodies corporate;
- notification requirements; and
- the role of the Privacy Commissioner and the need for Office of the Privacy Commissioner (OPC) guidance.[21]

11.15 The ALRC examined the application of section 5B of the Privacy Act to agencies and formed the view that while section 5B applies only to organisations:

> Agencies often compel the collection of personal information and should therefore remain accountable for the handling of that information under the Privacy Act, whether they are located in Australia or offshore. Further, agencies should not be able to avoid their obligations under the Act by transferring the handling of personal information to entities operating in countries with lower privacy protection standards.[22]

The ALRC therefore recommended that agencies that operate outside Australia should be subject to the Privacy Act.

11.16 One of the criticisms of NPP 9 is that organisations, which transfer personal information to recipients in foreign countries, are not held accountable for subsequent breaches of privacy. Given the risks associated with cross-border transfers, and the significant community concern around the issue, the ALRC suggested it was pertinent that agencies and organisations which transfer information to a recipient outside of Australia be held accountable for the acts and practices of the recipient in respect of

---

20 Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*, p. 89; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1084–85.

21 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1066.

22 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1082–1084 and 1104.

the transferred personal information.[23] The ALRC specified three circumstances in which an agency or organisation should not be held liable namely, where the:

- information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the UPPs;
- individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
- agency or organisation is required or authorised to transfer the personal information by or under law.[24]

11.17 The ALRC noted the concerns of stakeholders with respect to the 'reasonably believes' test currently used in NPP 9(a). However, the ALRC recommended that the test be retained, and that the Government issue a list of 'laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar' to those in Australian legislation, to assist agencies and organisations with compliance. The factors to be considered in determining whether an entity has a 'reasonable belief' may include 'the level of enforcement of a relevant law, binding scheme or contract, which may not be answered solely by their inclusion on the proposed list'. Therefore, the ALRC also suggested that the OPC issue guidance on what constitutes a 'reasonable belief'.[25]

11.18 Noting that provision of consent under this principle has significant implications, the ALRC suggested that the application of more detailed consent requirements than the usual 'voluntary and informed', may be required. For example, an agency or organisation may need to be able to demonstrate that informed consent was obtained, possibly through a written acknowledgement. Further, in order to provide informed consent, an individual would need to be notified of the countries to which their information may be sent. Such information could be included in a privacy policy, and the notification requirements under the principles would apply in this circumstance. The ALRC recommended that the OPC provide guidance on what is required of agencies and organisations in obtaining an individual's consent in particular contexts under the Privacy Act.[26]

---

23 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1087–97.

24 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1095–96.

25 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1097–1100.

26 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1103–04.

11.19 The views of submitters to the ALRC review were widely varied on the definition of the term 'transfer' and whether a definition should be provided in the legislation. Given the disparity in views, the ALRC recommended that the OPC issue guidance on the circumstances in which a cross-border transfer would occur, as such guidance 'can more readily be amended to accommodate changes to the ways in which personal information is transferred than a definition of "transfer" under the Privacy Act'.[27]

11.20 Stakeholders noted that under the current legislation it is not clear whether the transfer of personal information outside of Australia to a related body corporate is subject to NPP 9, due to the interaction between this principle and subsection 13B(1). Subsection 13B(1) states that the collection or disclosure of non-sensitive personal information between two related bodies corporate is not an interference with the privacy of an individual. The ALRC formed the view that it is in the public interest for the principle relating to the cross-border transfer of information to apply to transfers of information by organisations to related bodies corporate outside of Australia, as:

> Although many related companies are governed by a common set of internal policies, this may not always be the case. Further, the internal policies of a related company may not always provide the same level of protection as the Privacy Act.[28]

11.21 The ALRC noted that while the 'ability to investigate breaches of local privacy laws in foreign countries poses particular challenges for privacy regulators', the OPC and the Australian Government are already cooperating with privacy regulators in other jurisdictions in various forums.[29]

11.22 Most submitters to the ALRC review stated that an individual should be notified if their personal information will be transferred outside of Australia. However, the ALRC formed the view that a notification each time an individual's information is transferred overseas would be an onerous and unjustified compliance burden on agencies and organisations. The ALRC suggested that it would suffice if:

- the entity's privacy policy set out whether the entity may transfer personal information outside of Australia, and list those countries to which the information may be transferred; and
- under the 'notification' principle, an individual would be notified if their personal information may be transferred overseas.[30]

---

27 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1114–17.

28 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1117–19.

29 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1123.

30 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1127–29.

Government response

11.23 The Government accepted seven of the eight ALRC recommendations in relation to cross-border data flows and accepted with amendment the recommendation relating to exceptions.[31]

11.24 In relation to exceptions, the Government accepted that, as a general principle, an agency or organisation should remain accountable for the information which they transfer outside of Australia. The Government was also of the view that there should be certain exceptions to this general principle, agreeing with two of the exceptions proposed by the ALRC, namely the consent exception and the required or authorised by or under law exception. However, the Government considered the exception under which an agency or organisation reasonably believes the recipient is subject to substantially similar privacy protections should be amended to ensure that there are also enforceable mechanisms to enable individuals to take action if there is a breach of their privacy. The Government suggested that these enforcement mechanisms:

> ...may be expressly included in the law or binding scheme or may take effect through the operation of cross-border enforcement arrangements between the Office of the Privacy Commissioner and an appropriate regulatory authority in the foreign jurisdiction.[32]

11.25 The Government also considered that there should be further exceptions to the general principle of accountability, as follows:

- there is a reasonably belief that the disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety; or public health or public safety and in the circumstances, it is unreasonable or impracticable to seek the individual's consent;
- there is reason to suspect that unlawful activity or serious misconduct has been, is being, or may be engaged in, and the disclosure of the personal information is a necessary part of the entity's own investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- there is a reasonably belief that the disclosure is necessary for 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.[33]

11.26 The Government response further stated that individuals should be notified if their personal information is reasonably likely to be transferred overseas, and if so, to

---

31 Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, pp 77–80.

32 Australian Government, *Enhancing National Privacy Protection*, pp 77–78.

33 Australian Government, *Enhancing National Privacy Protection*, p. 78.

which locations it might be transferred. The Government envisaged this requirement would be provided for under the 'notification' principle, and would be qualified by the 'reasonable steps' test (see chapter 8).[34]

Issues

11.27 The Australian Institute of Credit Management welcomed APP 8 as it believed it will 'significantly ameliorate concerns regarding the management of personal information in the international context'.[35] However, Professor Greenleaf and Mr Waters called APP 8 'the most controversial new principle' as it abandons a 'border protection' approach in favour of an 'approach mis-described as "accountability"'.[36] Privacy NSW considered that the principle should be more stringent than the use or disclosure principle (APP 6) and disclosure should only take place outside Australia where the same level of protection as the APPs is afforded or if there is express consent.[37]

11.28 Other submitters stated that APP 8 increased the compliance burden on organisations, while the Australian Hotels Association commented that this was a further regulatory requirement on an essential business process.[38] Yahoo!7 on the other hand, preferred that accountability for the handling of cross-border data disclosure be through self regulatory codes and cooperative instruments and commented 'whilst we appreciate the need to provide information and reassurance to users in relation to cross-border transfers, we consider any reliance on distinction between borders to be unrealistic'.[39]

11.29 The following discussion addresses concerns in relation to the accountability for personal information transferred overseas, the structure of APP 8, the exceptions to the principle and interaction between APP 8 and section 20.

Accountability for personal information transferred overseas

11.30 The NSW Department of Justice and Attorney General commented that APP 8 itself does not embody the principle of entities remaining accountable for personal information transferred to an overseas recipient. Rather, the principle only provides for a 'reasonable steps' test and the 'accountability' principle is contained in

34 Australian Government, *Enhancing National Privacy Protection*, p. 81.

35 Australian Institute of Credit Management, *Submission 8*, p. 4.

36 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

37 Privacy NSW, *Submission 29*, p. 5.

38 Australian Hotels Association, *Submission 22*, p. 3; Communications Council, *Submission 23*, p. 9.

39 Yahoo!7, *Submission 20*, p. 3.

proposed section 20.[40] The NSW Department of Justice and Attorney General submitted that, for clarity, the accountability principle could be embodied in the APP and not in a separate section of the Act. It was suggested that, at the very least, a note could be included following APP 8 to indicate that the accountability principle applies and stating its location. This would avoid the risk that entities or individuals assuming that APP 8 is exhaustive in relation to cross-border transfers and that the only obligation on entities is to take reasonable steps to ensure that the overseas recipient does not breach the APPs. The NSW Department of Justice and Attorney General went on to submit that compliance only with APP 8 would provide a far more limited safeguard than the accountability principle that appears in section 20.[41] The OPC also supported the inclusion of a note referring to section 20.[42]

11.31 In relation to the change to an 'accountability model', the Australian Bankers Association (ABA) supported APP 8 using such a model as 'it is commercially and socially realistic'.[43] While Google supported the approach in the principle, it voiced concern with the strict liability imposed by section 20.[44] Other submitters also expressed concern about the shift in liability. The Australian Finance Conference (AFC) commented that the principle shifts the risk balance heavily to the entity and queried 'the individual interest justification to support that'. It commented that APP 8 departs from the ALRC recommendations and from the current NPP 9. The AFC also questioned the approach taken in APP 8 given Australia's recent commitment to the APEC Cross-border Privacy Enforcement Arrangement (CPEA). The APEC CPEA is aimed at assisting in the removal of country boundaries in the enforcement of privacy protections.[45]

11.32 Microsoft also raised the CPEA and commented that the combination of APP 8 and section 20 'appears to go further than both the APEC accountability principle and the government's own response to the ALRC recommendations' as the entity will be liable if the recipient outside Australia acts inconsistently with the APPs. Microsoft commented that 'liability will be imposed even where the Australian entity exercised due diligence and took reasonable steps to ensure that the recipient would abide by the principles'.[46]

---

40 As described in paragraph 11.5 above, section 20 makes an entity accountable for the overseas recipient's acts and practices and a breach of the APPs by the overseas recipient will be taken to be that of the entity who disclosed the personal information to the overseas recipient. Companion Guide, p. 13.

41 NSW Department of Justice and Attorney General, *Submission 42*, p. 8.

42 Office of the Privacy Commissioner, *Submission 39*, p. 36.

43 Australian Bankers' Association, *Submission 15*, p. 11.

44 Google, *Submission 16*, p. 7.

45 Australian Finance Conference, *Submission 12*, pp 7–8.

46 Microsoft, *Submission 14*, p. 11; see also Australian Bankers' Association, *Submission 15*, p. 11.

11.33 Deloitte Australia commented on the point raised by Microsoft and suggested that the interaction between section 20 and APP 8 was unclear. Although it supported the accountability principle, Deloitte suggested that the disclosing entity should only be liable under section 20 if it did not take reasonable steps as required under APP 8(1). It also noted the comments of the ALRC in relation to information that is the subject of a contract that effectively upholds privacy protections substantially similar to the UPPs and the provisions of the CPEA.[47]

11.34 The Law Council of Australia (LCA) also commented that the onus placed on entities is stricter than that under the CPEA. The LCA suggested that section 20 is unnecessary if the provisions of APP 8 have been complied with.[48]

11.35 In response to comments in submissions about the intention of the principle, and the shift to an accountability framework, the Department of the Prime Minister and Cabinet (the department) stated that the Government had accepted the general principle that an agency or organisation should remain accountable for personal information that is transferred outside Australia. The Government also accepted that there should be a limited number of exceptions to the principle and that the term 'accountable' should be defined so that the scope of the principle is clear to agencies and organisations.[49]

11.36 The department went on to note that the key instrument considered in developing the principle was the CPEA, which in turn is derived from the OECD principles. The key element of accountability is that an agency or organisation transferring personal information should exercise due diligence and take reasonable steps to ensure the recipient will protect the personal information.

11.37 In addition, one way to meet a requirement that a foreign recipient protect personal information would be to use a contract. The department noted that while contracts will remain useful as important mechanisms for agencies and organisations to impose obligations upon recipients, they should not provide a specific exception on their own from the accountability obligations. It is expected that entities will ordinarily have a contractual relationship with overseas recipients, and that contract would set out the obligations of the overseas recipient. This may not be reasonable in all circumstances but it is the general expectation.[50]

11.38 Matters specific to section 20 are discussed below, see paragraphs 11.121–134.

---

47 Deloitte Touche Tohmatsu, *Submission 28*, pp 1–2.

48 Law Council of Australia, *Submission 31*, p. 6.

49 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 24.

50 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 24.

Conclusion

11.39 The committee acknowledges that APP 8 and section 20 address the growing community concerns that technology allows information to be shared freely across borders. While the committee notes concerns about the liability imposed by section 20, even when reasonable steps have been taken by the entity, the department and the Companion Guide explained that this will be managed through contractual relationships with the overseas recipients including privacy obligations. Therefore the committee does not consider that the obligations imposed by APP 8 and section 20 are overly onerous.

11.40 In line with the committee's previous comments in relation to clarity, the committee considers that a note referring to section 20 should be included in APP 8 to ensure that the interaction between both provisions is clear.

Recommendation 14

11.41 The committee recommends that a note be added to the end of APP 8 making reference to section 20 of the new Privacy Act.

Notification

11.42 Professor Graham Greenleaf and Mr Nigel Waters commented that as currently drafted, APP 8 does not appear to require notification of individuals at the time that their data is being transferred to an overseas jurisdiction. They considered that this compounded their concerns raised in relation to APP 1 and APP 5 relating to notification of an individual of the countries to which their personal information may be disclosed.[51]

11.43 The committee notes, that in its review, the ALRC recognised that individuals should be notified if their personal information is to be transferred outside of Australia. However, it was noted that requiring a notification each time an individual's information is transferred overseas would be an onerous compliance requirement for agencies and organisations.[52] The Government agreed with the ALRC's recommendation that an agency or organisation's privacy policy should state whether personal information is likely to be transferred overseas, and where it may be transferred to. The Government also stated in its response that a requirement to notify individuals of the possible transfer of their personal information overseas would be expressly provided for in the 'notification' principle, but would be qualified by a 'reasonable steps' test:

> For example, an agency or organisation would not need to include this information in a collection notice if it did not reasonably know at the time of collection whether information would be transferred overseas.

51 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

52 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1127–29.

> Further, it would not be reasonable to provide specific information if the organisation or agency does not reasonably know to which specific jurisdiction personal information may be transferred.[53]

Structure and terminology

11.44 In relation to structure and terminology used in APP 8, the Office of the Victorian Privacy Commissioner (Privacy Victoria), suggested that including exceptions which relate solely to Commonwealth agencies in privacy principles which are supposed to be 'high-level' is problematic, as it increases complexity and makes the principles less readily transferable to states and territories.[54] The AFC also submitted that, as a matter of policy and drafting, APP 8 fails to achieve the key objectives of the privacy reforms of high-level, simple, clear and easy to understand principles.[55]

11.45 Privacy Law Consulting Australia raised various concerns regarding the terminology used in the exposure draft of APP 8. In relation to APP 8(1), it was noted that the APPs do not apply to overseas recipients, therefore phrasing similar to section 20(1)(d) should be included in the provision, such as 'if those Australian Privacy Principles applied to it'.[56]

11.46 The committee has commented on general matters in relation to clarity and agency specific provisions in chapter 3.

To 'transfer' or to 'disclose'

11.47 APP 8 uses the term 'disclosure' rather than 'transfer' as is currently used in NPP 9. The Companion Guide states that the term 'transfer' complicates the understanding of the information flow. Rather, the ordinary meaning of disclosure is to allow information to be seen rather than the implication of 'transfer' of a cross-border movement of information. This means that a disclosure will occur when an overseas recipient accesses information, whether or not the personal information that is accessed is stored in Australia or elsewhere. The APP will not apply if the information is routed through servers outside Australia.[57]

11.48 Telstra raised concern about the meaning of 'accessed' by an overseas recipient. While agreeing that the principle should apply in the case where an overseas recipient is able to have possession of personal information, Telstra argued that the principle should not be extended to cover situations in which the information is

---

53 Australian Government, *Enhancing National Privacy Protection*, p. 81. See chapter 8 for further information.

54 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 8.

55 Australian Finance Conference, *Submission 12*, p. 8.

56 Privacy Law Consulting Australia, *Submission 24*, p. 9.

57 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

temporarily 'viewed' by an overseas recipient who cannot print, copy or save the information. In Telstra's opinion, the entity which possesses the information should remain responsible for the management of that information.[58]

11.49 The Financial Services Council (FSC) noted the explanation provided in the Companion Guide, which outlines that information will not be taken to be 'disclosed' if it is routed through servers which are outside of Australia or stored offshore. However, it was submitted that these intentions should be clarified in APP 8 and the provisions of the Privacy Act itself, and explanatory material should also clearly state that entities will need to ensure that information routed or stored offshore is not accessed by third parties, and thereby 'disclosed'.[59]

11.50 The OPC suggested concerns about the use of the term 'disclosure' could be addressed by including explanatory material to note that APP 8 and related provisions only apply to disclosures and not to an entity's internal 'uses'.[60] The OPC also suggested that explanatory material clarifying that APP 8 will apply to disclosures to a 'related body corporate' be included, consistent with recommendations in the ALRC report, and as accepted in the Government's response.[61]

11.51 In relation to the intention that the principle will not apply to information routed through servers outside Australia, the OPC commented that it agreed with this view 'provided the personal information is not accessed by a third party during this process'. The OPC concluded:

> The Companion Guide or other explanatory material could note that entities will need to take a risk management approach to ensure that personal information routed overseas is not accessed by third parties. If the information is accessed by third parties, this will be a disclosure subject to APP 8 (among other principles).[62]

Conclusion

11.52 In light of the comments received by the committee in relation to the 'disclosure' of personal information, the committee considers that greater clarity is required around the use of this term. The committee is of the view that explanatory material should be prepared that clearly outlines when information is taken to be 'disclosed' through cross-border activities. The committee also considers that explanatory material regarding the application of APP 8 to disclosures to a 'related body corporate' should be provided.

---

58 Telstra Corporation Limited, *Submission 19*, p. 3.

59 Financial Services Council, *Submission 34*, p. 3; see also Office of the Privacy Commissioner, *Submission 39*, p. 37.

60 Office of the Privacy Commissioner, *Submission 39*, p. 37.

61 Office of the Privacy Commissioner, *Submission 39*, p. 37.

62 Office of the Privacy Commissioner, *Submission 39*, p. 37.

Recommendation 15

11.53 The committee recommends that the Department of the Prime Minister and Cabinet develop explanatory material to clarify the application of the term 'disclosure' in Australian Privacy Principle 8.

Ensuring an overseas recipient does not breach the APPs–APP 8(1)

11.54 APP 8(1) requires an entity, which is disclosing personal information to an overseas recipient, to 'take such steps as are reasonable in the circumstances' to ensure that the overseas recipient does not breach the APPs in relation to the information before the disclosure takes place.

11.55 The LCA submitted that this is an onerous requirement as in order to achieve the aim of APP 8(1) an Australian entity would have to require the overseas entity to bind itself to observe the APPs and the affected overseas entity may resist. The LCA suggested an amendment to the provision so that the Australian entity must take reasonable steps to ensure that the foreign recipient does not hold, use or disclose personal information 'in a manner inconsistent with the Australian Privacy Principles'.[63]

11.56 Qantas expressed concern that the requirement to 'ensure that the overseas recipient does not breach the Australian Privacy Principles' is too broad, suggesting that the approach taken in NPP 9(f), which requires the overseas recipient to hold, use and disclose the personal information in a manner consistent with the APPs, is more appropriate.[64]

11.57 Some submitters commented that APP 8 is complex and confusing, as there is no explanation of what might constitute 'reasonable steps'.[65] Professor Graham Greenleaf and Mr Nigel Waters noted that in the absence of a definition of what might constitute reasonable steps, guidelines from the Australian Information Commissioner are essential. It was further noted that guidance on model contract clauses will make it easier to determine whether a contract meets the 'reasonable steps' compliance test in APP 8(1).[66]

11.58 Dr Colin Bennett argued APP 8 does not explicitly state the intention of the principle, which, as explained in the Companion Guide is that, 'if the overseas recipient does an act or practice that would be a breach, then the entity would be liable'. Dr Bennett suggests that Canadian privacy legislation states the entity's responsibility more clearly, and encourages an organisation to use contractual

63 Australian Law Council, *Supplementary Submission 31a*, p. 4.

64 Qantas, *Submission 38*, pp 7–8.

65 Dr Colin J. Bennett, *Submission 11*, p. 4; Internet Society of Australia, *Submission 41*, p. 3; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

66 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

arrangements to ensure the adequate level of privacy protection is complied with by the third party.[67]

11.59 Coles Supermarkets Australia Pty Ltd (Coles) supported this argument and explained that when outsourcing services, Coles puts contracts in place which oblige the overseas recipient to manage personal information in accordance with the requirements of Australian privacy laws, and provide that the service provider's compliance with the contract may be audited. Coles suggested that similar requirements could be applied under the principles to any third party recipients of personal information, regardless of their location.[68]

11.60 However, in its submission the ABA recognised that it is stated in the Companion Guide that it is generally expected that entities will use contractual arrangements to ensure that an overseas recipient manages information in a manner which is consistent with the APPs, and that the existence of such contractual arrangements indicates that an entity has taken reasonable steps as required.[69]

11.61 Guidance on the term 'reasonable steps', is provided in the *Guidelines to the National Privacy Principles* produced by the OPC, and it is expected that similar guidance will be issued for the APPs. Professor Rosalind Croucher, President of the ALRC, explained that the Office of the Australian Information Commissioner:

> ...might assist in the process of determining what is reasonable, in conjunction with the kinds of other steps that we have suggested before. There are other sources of best practice. The advantage of an information commissioner's office is that it is a central repository and a high-level federal government agency that can assist in the process of making these high-level principles more operationally effective in the interests underpinned by the principles.[70]

11.62 Further, the Government response supported the ALRC's suggestion that the OPC provide guidance on what should be contained in a contractual agreement with an overseas recipient of personal information.[71]

Conclusion

11.63 The committee considers that, as the Government envisages that most Australian entities and overseas recipients will have contractual arrangements in place which will be used to ensure information is managed in accordance with Australian privacy law, guidance should be provided to assist entities in this regard. In addition,

---

67 Dr Colin J. Bennett, *Submission 11*, p. 4.

68 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 2.

69 Australian Bankers' Association, *Submission 15*, p. 12.

70 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 9.

71 Australian Government, *Enhancing National Privacy Protection*, p. 80.

compliance with APP 8(1) contains a 'reasonable steps' test. Therefore the committee considers that, as a matter of priority, the Office of the Australian Information Commissioner should provide guidance in relation to the type of contractual agreements required to comply with APP 8.

Recommendation 16

11.64 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the types of contractual arrangements required to comply with APP 8 and that guidance be available concurrently with the new Privacy Act.

Exceptions

11.65 APP 8(2) sets out a number of exceptions under which an entity will not be accountable for the cross-border disclosure of personal information to an overseas recipient. As the cross-border disclosure of personal information has been extended to agencies, a number of agency specific exceptions have been included to 'ensure that current information sharing activities of agencies is still permitted'.[72] Comments on the inclusion of agency specific exceptions are contained in chapter 3.

11.66 Professor Greenleaf and Dr Waters argued that the 'attempt at regulation of overseas transfers' through APP 8(1) is 'fatally undermined by APP 8(2) which provides nine separate means by which a data exporter can be exempt from even the theoretical liability/"accountability" of APP 8(1)'.[73] The following canvasses the issues raised in relation to specific exceptions.

Similar overseas laws and enforcement mechanism exception–APP 8(2)(a)

11.67 APP 8(2)(a) provides that if the entity transferring personal information overseas 'reasonably believes' that the recipient of that information is subject to laws which protect the information in a way that is at least substantially similar to the APPs and there are accessible mechanisms available to enforce those protections, an exception to the provisions of APP 8(1) is available.

11.68 Microsoft noted the Government's response to the ALRC's recommendations extended the exception to include the accessible enforcement mechanisms for individuals to be able to take effective action to have the privacy protections enforced. The Government response stated that any such enforcement mechanism may be expressly provided for in a law or binding scheme, or be given effect through cross-border enforcement arrangements between the OPC and an appropriate foreign regulator. Microsoft submitted that it did not consider that proposed APP 8(2)(a) reflects the position stated in the Government response. Microsoft suggested that the exception be redrafted to ensure that:

---

72 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

73 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

- the foreign recipient is in a jurisdiction with an adequate level of protection;
- the foreign recipient is in a jurisdiction that has entered into a cross-border enforcement arrangement with the OPC that will enable an individual to pursue a claim against the foreign recipient in respect of conduct that would constitute an interference of privacy if it had occurred in Australia.[74]

11.69 A number of other issues were raised in relation to this exception. On the one hand, privacy commentators considered that the exception was flawed while data exporters pointed to the compliance burden.

11.70 Professor Greenleaf and Mr Waters argued that APP 8(2) was weakened by the inclusion of the term 'reasonably believes' and submitted that:

> Some organisations will inevitably make self-serving judgements about the level of protection in other jurisdictions and/or pay for advice that supports their desire to transfer. Similar protection should be an exception to any prohibition on transfer, but it must be based on objective criteria.[75]

11.71 As a consequence, they recommended that the term 'the entity reasonably believes that' be deleted, 'so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal'. Professor Greenleaf and Mr Waters concluded that 'such ex post facto determinations may discourage exports of Australians' personal information to countries where privacy protection is questionable, but that would be a good result'.[76]

11.72 Dr Colin Bennet was of a similar view: either the overseas recipient is subject to a law or binding scheme similar to the Australian legislation, or it isn't, and noted that entities could use this to avoid liability in cases where they have not exercised due diligence.[77]

11.73 Submitters raised concerns in relation to the compliance burden and access to a comprehensive list of destinations which have regimes so that an entity could comply with APP 8(2)(a). Qantas, for example, submitted that the requirements of APP 8(2)(a) relating to the availability of enforcement mechanisms is 'too onerous for an Australian entity to comply with and should be removed'.[78] In addition, it was argued that if entities were required to make their own determination, a situation could

74 Microsoft, *Submission 14*, p. 11.

75 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

76 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

77 Dr Colin J Bennett, *Submission 11*, p. 4.

78 Qantas, *Submission 36*, p. 8; see also Telstra Corporation Limited, *Submission 19*, pp 3–4.

arise whereby different entities make different determinations about the level of privacy protection available in various jurisdictions.[79]

11.74 Submitters called for the provision of a list which identifies countries with similar privacy laws to Australia and which have accessible protection mechanisms. Submitters suggested that the OPC should compile and publish a list while Microsoft suggested that this should be a 'positive obligation' on the OPC.[80] Such as list would ensure consistent treatment of privacy protection between entities and would assist entities in complying with their obligations, particularly under APP 8(2)(a) when disclosing information offshore.[81] It was noted that some international jurisdictions have adopted this approach in relation to Anti-Money Laundering legislation, and that the compilation of such a list may be facilitated by the new APEC Cross-border Privacy Enforcement Arrangement.[82]

11.75 The NSW Department of Justice and Attorney General also commented that the NSW Law Reform Commission's view was that, if such a list is published, there is no need for the reasonable belief test. Further, such a list could include not only laws but also 'binding schemes' such as inter-governmental agreements or effective self-regulatory schemes. The NSW Department of Justice and Attorney General stated:

> There is a question about the circumstances in which an entity could hold the necessary "reasonable belief" in relation to an entity in a jurisdiction not on the list. It is conceivable that a jurisdiction with adequate protection might not be on the list due to delays in maintaining the list. In such circumstances, the reasonable belief test could provide a safety net for entities. However, provided the list is effectively created and maintained, in the vast majority of cases a belief is unlikely to be 'reasonable' in relation to an entity in a non-listed jurisdiction.[83]

11.76 The NSW Department of Justice and Attorney General further commented that a belief may be reasonable, based on the information available to an entity, but it may be ill informed and incorrect. It concluded that removal of the 'reasonable belief' exception in favour of the 'listed jurisdiction' approach, as recommended by the NSW Law Reform Commission may be worth further consideration.[84]

---

79 Telstra Corporation Limited, *Submission 19*, p. 4.

80 Microsoft, *Submission 14*, p. 12.

81 The Westpac Group, *Submission 13*, p. 3; Australian Bankers' Association Inc., *Submission 15*, p. 13; Telstra Corporation Limited, *Submission 19*, pp 3-4; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14; Deloitte Touche Tohmatsu, *Submission 28*, p. 2.

82 The Westpac Group, *Submission 13*, p. 3; Internet Society of Australia, *Submission 41*, p. 3; Telstra Corporation Limited, *Submission 19*, pp 3–4.

83 NSW Department of Justice and Attorney General, *Submission 42*, p. 9.

84 NSW Department of Justice and Attorney General, *Submission 42*, p. 9.

11.77 The ALRC review recognised concerns regarding the 'reasonably believes' test which is used in existing NPP 9(a), but recommended that the test be retained. To assist agencies and organisations with compliance, the ALRC suggested the Government issue a list of laws and binding schemes which are substantially similar to the protections provided under Australian legislation. However, the ALRC noted that the level of enforcement of a relevant law or binding scheme would not be reflected by inclusion on a list. For example, entities may know that there is no mechanism for enforcement of privacy protection laws and thus could not demonstrate 'reasonable belief' for the purposes of the principle. The ALRC suggested that the OPC issue guidance on the 'cross-border data flows' principle which should include what constitutes a 'reasonable belief'.[85]

11.78 In its response to issues raised in relation to this exception, the department noted that 'the ALRC made it clear that the mere fact that a recipient is subject to a listed binding law or scheme is not determinative in itself, as the entity must still form its own reasonable belief based on the information available to it'. Further, the Government response stated that agencies and organisations will be able to use the list to assist them in forming a reasonable belief that, in the circumstances of their particular cross-border transfer of personal information, the recipient of the information will be accountable. The department commented:

> Once armed with the initial information, entities would be in the best position to find out about the specific laws that apply to the overseas recipient, including whether the recipient is bound by existing privacy laws in the overseas jurisdiction that are substantially similar (we understand that some privacy laws, for example in Korea, only apply to certain industry sectors).[86]

11.79 The department noted that the list would be prepared by the Government rather than the Office of the Australian Information Commissioner.[87]

11.80 The enforcement mechanism requirement was also examined by the LIV from the perspective of access by affected individuals. While mechanisms may exist, the LIV commented that if it is time consuming, costly, or not applied in a practical sense 'then it does not provide any meaningful protection to individuals' and 'it is unrealistic to expect Australian citizens to avail themselves of such mechanisms'.[88] PIAC and the Health Services Commissioner similarly argued that the affected individual should not have to take action in another jurisdiction against a third party in order to protect the rights afforded by Australian privacy law. Rather, the individual should always be

---

85 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1097–1100.

86 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 25.

87 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 25.

88 Law Institute of Victoria, *Submission 36*, p. 7.

able to take action in Australia and against the entity with which he or she had direct dealings.[89]

Consent to cross-border disclosure–APP 8(2)(b)

11.81 APP 8(2)(b) provides that APP 8(1) does not apply if the entity obtains the consent of the individual to overseas disclosure, after the individual has been given information to that effect. Submitters raised two matters: the practicality of the consent requirement in relation to commonplace international transactions; and the lack of the need to gain 'express' consent.

11.82 The ABA noted that there are a wide range of quite common international transactions, such as international payments and international credit card transactions, in which it is clear that information will cross international borders. The ABA stated that it is not practicable to impose controls on recipients in such transactions, and consequently, its members will find it difficult to meet the requirements under APP 8(2)(b). To address this issue, the ABA suggested an additional exception be provided under APP 8(2) for circumstances in which the:

> ...overseas transfer of information is a necessary step in providing a service which would be obvious to a reasonable person turning their mind to the circumstances.[90]

11.83 The ABA submitted that if a bank is required to expressly inform each individual customer separately that their information will be disclosed to an overseas recipient, 'the consent exception will, in all practicality, be illusory'. Consequently, the ABA suggested that an individual can be expressly informed by an entity through the provision of information in the entity's privacy policy, so that the customer is aware that in continuing to deal with the entity, they consent to the potential for their information to be sent to an overseas recipient.[91]

11.84 However, the possibility that entities would use privacy statements to meet the consent requirement was of concern to other submitters. Professor Greenleaf and Mr Waters commented that there was no requirement to explain the 'risk' either generally or in relation to a specific destination. As consent can be implied, entities may rely on 'small print' notices in standard terms and conditions statements which were 'completely ineffective'.[92]

11.85 The issue of 'implied' consent through a notice being included in a privacy statement was raised by other submitters.[93] The Health Services Commissioner,

---

89 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 3; Public Interest Advocacy Centre, *Submission 32*, p. 1, Attachment, pp 12–13.

90 Australian Bankers' Association, *Submission 15*, p. 12.

91 Australian Bankers' Association, *Submission 15*, pp 12–13.

92 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15, Attachment, p.15.

93 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 3.

Victoria, argued that a detailed privacy notice at the end of a document which includes information about disclosures overseas 'is not likely to be read by many individuals'. In addition, more stringent requirements are needed in relation to sending health information overseas.[94] The LIV suggested that if this provision is retained, it should incorporate a requirement that such consent be 'free, express and fully informed' to ensure that any such consent is not implied.[95] Professor Greenleaf and Mr Waters suggested that the provision be amended so that individuals, who consent, be provided with a written notice that contains the information provided to the individual when the consent was given.[96]

11.86 In its review, the ALRC considered that the application of more detailed consent requirements than the usual 'voluntary and informed', may be required under this principle as provision of consent in these circumstances has significant implications. Consequently, the ALRC recommended that the OPC provide guidance on what is required of agencies and organisations in obtaining an individual's consent to the transfer of their information overseas. This recommendation was accepted by the Government.[97]

11.87 The ALRC's position on the concept of consent was explained more fully by Professor Rosalind Croucher, President of the ALRC at the committee's public hearing:

> In our report we recommended that the Office of the Privacy Commissioner should develop and publish guidance about what is required of agencies and organisations to obtain an individual's consent. This guidance should, for instance, address a number of the things that I am grabbing at—the factors to be taken into account by agencies and organisations in assessing whether it has been obtained, which is kind of what you are asking about in asking how. It should cover express and implied 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—in other words, a consent to general use. So we do consider that in the report. I suppose the simple answer is that it depends on the context, but we have suggested that the Office of the Privacy Commissioner, which now sits under the Information Commissioner's office, might be the appropriate agency through which such guidance could be developed.[98]

---

94 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 3.

95 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 8; see also Privacy NSW, *Submission 29*, p. 5.

96 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15, Attachment, p.15.

97 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1103–04; Australian Government, *Enhancing National Privacy Protection*, p. 80.

98 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 7.

Required or authorised by or under and Australian law–APP 8(2)(c)

11.88 Google Australia Pty Limited (Google) suggested that APP 8(2)(c) only covers disclosures to an overseas recipient, not any subsequent disclosure by that recipient which may be required by law in the overseas jurisdiction. It was argued that the provision should recognise requirements of foreign law to ensure that Australian entities are not put at risk of being in breach of the Act under section 20, due to a disclosure of personal information by an overseas recipient required by a foreign law.[99]

11.89 However, the committee notes that the Companion Guide indicates that subsection 6A(4) and section 13D of the current Privacy Act, provide that if an act or practice which is done or engaged in outside Australia is required by an applicable law of a foreign jurisdiction, then that act or practice is not deemed to be an interference with privacy. The Companion Guide states that these provisions are to be replicated in the new Act and will cover agencies.[100] In addition, the department responded to Google's concerns and reiterated that the existing policy achieved by subsection 6A(4) and section 13D of the Privacy Act will be retained in the amended Act. In the example provided by Google, an Australian entity would not breach the APPs if an applicable foreign law required disclosure of personal information by an entity to which that information had been disclosed.[101]

Required or authorised by or under an international agreement–APP 8(2)(d)

11.90 APP 8(2)(d) provides an exception if an entity is an agency and the disclosure of the information is required by or authorised by or under an international agreement related to information sharing, and Australia is a party to that agreement. Concerns were raised by the LIV that compliance with the APPs may be avoided by government by entering international agreements. The LIV stated 'we note that there is no regulation or requirement that international agreements about information sharing comply with the APP' and provided the example of the ease with which governments can circumvent the APPs through international agreements by pointing to the Department of Immigration and Citizenship's agreement with five countries to exchange biometric information in relation to protection visa applicants.[102] Professor Greenleaf and Mr Nigel Waters went further and called this 'policy laundering', that is 'hiding behind often spurious claims of "international obligations" to justify actions which would not otherwise be lawful'.[103]

99 Google Australia Pty Limited, *Submission 16*, pp 7–8.

100 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 7.

101 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 25.

102 Law Institute of Victoria, *Submission 36*, p. 7.

103 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15.

11.91 The OPC expressed similar concerns that the scope of the exception was unclear and could be quite widely interpreted, thereby limiting the circumstances in which an agency can be held accountable for the disclosure of personal information overseas. The OPC explained that wherever practicable 'specific domestic legislative authority should be the basis for an agency to disclose personal information under an international agreement relating to information sharing' thereby providing clarity and certainty to agencies and ensuring that information sharing practices by agencies are subject to appropriate parliamentary scrutiny. If no such legislative authority exists, the OPC suggested the disclosure of information should be subject to other forms of scrutiny, 'such as through a public interest determination (a legislative instrument) issued by the Privacy Commissioner'.[104]

11.92 With regard to this exception, OPC suggested the committee:

- seek further advice on the range of international agreements that may be encompassed by the exception; and
- consider whether those agreements are subject to sufficient parliamentary scrutiny, such that it is appropriate for APP 8 to permit disclosures that are authorised by those agreements (rather than relying on the 'required or authorised by law' exception in APP 8(2)(c)).[105]

11.93 The Companion Guide states that the exception allowing cross-border disclosure of information pursuant to information sharing under an international agreement, was necessary to include as the cross-border disclosure principle has been extended to cover agencies. This exception will facilitate the current information sharing activities of agencies.[106]

Law enforcement activities–APP 8(2)(g)

11.94 An exception is available to agencies for the disclosure of information, to overseas bodies 'similar' to Australian enforcement bodies, where it is necessary for law enforcement activities by, or on behalf of, an Australian enforcement body. The OPC commented that the requirement that the overseas body performs functions, or exercises powers similar to those performed or exercised by the Australian body could be broadly interpreted. The OPC suggested that the term 'substantially similar' be used instead, as the definition of an enforcement body is strictly defined in section 15 of the exposure draft.[107]

104 Office of the Privacy Commissioner, *Submission 39*, p. 38.

105 Office of the Privacy Commissioner, *Submission 39*, p. 38.

106 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

107 Office of the Privacy Commissioner, *Submission 39*, pp 38–39.

Diplomatic, consular and defence activities–APP 8(2)(h) and APP 8(2)(i)

11.95 As noted in chapter 3, the OPC recommended that the diplomatic, consular and Defence Force activities exceptions be addressed in portfolio legislation rather than the Privacy Act, ensuring that these exceptions are only invoked where appropriate. Consequently the APPs would remain a broad high-level framework, applicable to all entities.[108]

Exceptions no longer included in the cross-border principle

11.96 The Law Council of Australia and Qantas noted that two exceptions which are currently provided for under the NPPs have not been included in APP 8. These relate to when the transfer of information is necessary under a contract (NPP 9(c) and (d)). In effect, the absence of these provisions means that:

> ...if an entity needs to disclose personal information which is necessary for the conclusion of the contract with an overseas entity which is not subject to a scheme which is similar to the APPs the entity will need to obtain consent or to enter into a contract which will ensure the overseas recipient does not breach the APPs.[109]

11.97 It was noted that this would be impracticable in a number of circumstances, particularly in sectors such as the travel industry. In such industries, entities commonly deal with overseas organisations with whom it is impracticable to enter into a contract, and situations in which it would not be possible to obtain an individual's consent at short notice. For these reasons, the Law Council and Qantas recommended that the NPP exceptions relating to the transfer of information required under a contract be included in the APPs.[110]

11.98 The department stated that in partially adopting ALRC recommendation 31-2, the Government accepted that it was not necessary to include an exception relating to fulfilling contractual obligations. In recommendation 31-2, the ALRC stated that, under the 'Cross-border Data Flows' principle, an exception to the concept of accountability should include where an 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. The department went on to state:

> The Government response to ALRC recommendation 31-2 stated that the application of contractual obligations on the recipient of the information does not provide an individual with any rights to take action under the contract. It went on to comment that, while contracts are important mechanisms for agencies and organisations to impose obligations upon

---

108 Office of the Privacy Commissioner, *Submission 39*, pp 28–30 and 39.

109 Law Council of Australia, *Submission 31*, p. 6; Law Council of Australia, *Supplementary Submission 31a*, p. 4; Qantas, *Submission 38*, pp 7–8.

110 Law Council of Australia, *Submission 31*, pp 6–7; Qantas, *Submission 38*, pp 7–8.

> recipients, they should not provide an exception from the general accountability obligations.
>
> Further, it is clear that in the case of existing NPP 9(c) and (d), which involves a contract between the individual and the organisation, or a contract concluded in the interest of the individual between the organisation and a third party, that the individual would consent to the transfer of the information. Under the new APP 8(2)(b), consent of the individual is an exception to the general prohibition under APP 8(1).[111]

Conclusions

11.99 The committee considers that it is reasonable to include exceptions to APP 8 in particular circumstances. The first exception, APP 8(2)(a), provides for an exception where similar law and enforcement mechanisms apply to the overseas recipients. The ALRC recognised that one of the more significant challenges faced by privacy regulators, is the ability to investigate breaches of local privacy laws in foreign countries. In light of this, the Government considered it appropriate that any law or binding scheme deemed to be substantially similar to the APPs must have effective enforcement mechanisms in order to be subject to the exception to the general accountability obligation. The Government suggested that such enforcement mechanisms could be specifically included in the law or binding scheme, or 'may take effect through the operation of cross-border enforcement arrangements between the Office of the Privacy Commissioner and an appropriate regulatory authority in the foreign jurisdiction.' The committee notes that the OPC and the Australian Government are already working to improve cooperative arrangements between privacy regulators across jurisdictions in a variety of forums including the CPEA.[112]

11.100 In relation to recommendations that a list of jurisdictions with similar privacy schemes be provided, the committee notes the department's comments that the list will be provided by the Government. However, the Government's expectation is that this will be 'initial information' and that entities will 'be in the best position' to find out about specific laws that apply to the overseas recipients they are dealing with. While the committee acknowledges that as it is the entity that is transferring the personal information overseas, it must be of a reasonable belief that the overseas jurisdiction provides for similar privacy protections, it may not always be possible for an entity to make such a judgment. The committee therefore considers that the Office of the Australian Information Commissioner should be available to assist entities in the interpretation of overseas privacy laws.

11.101 The committee considers that the 'consent' to cross-border transfers of personal information provides entities with a significant exception. As such, the

---

111 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 26.

112 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1123; Australian Government, *Enhancing National Privacy Protection*, pp 77–78.

committee considers that guidance on what constitutes consent particularly important and the Office of the Australian Information Commissioner should address this issue as a matter of priority. This matter is further discussed in chapter 3.

11.102 The committee has some concerns with the exception provided to agencies under APP 8(2)(d)–required or authorised by or under an international agreement. The committee considers that the scope of this exception is unclear and in addition, notes comments about its potential to undermine accountability and scrutiny. While the Parliament has formal mechanism to refer treaties to the Treaties Joint Standing Committee, this committee does not review sub treaty level agreements. The committee therefore considers that use of this exception by agencies should be subject to accountability mechanisms and parliamentary scrutiny.

Recommendation 17

11.103 The committee recommends that, when the Australian Government enters into an international agreement relating to information sharing which will constitute an exception under APP 8(2)(d), the agency or the relevant minister table in the Parliament, as soon as practicable following the commencement of that agreement, a statement indicating:

- **the terms under which personal information will be disclosed pursuant to the agreement; and**
- **the effect of the agreement on the privacy rights of individuals.**

11.104 In relation to the exception for law enforcement activities, the committee notes the OPC's concerns that APP 8(2)(g) could be interpreted broadly and suggests that the wording of this provision be revisited.

Recommendation 18

11.105 The committee recommends that further consideration be given to the wording of the law enforcement exception in APP 8(2)(g) to ensure that the intention of the provision is clear.

Extra-territorial application of the Privacy Act –section 19

11.106 Section 19 provides for the extra-territorial operation of the Act, that is the APPs will apply if the agency or organisation has an Australian link.

11.107 Google Australia Pty Limited (Google) agreed with the concept of 'Australian link' provided for in the exposure draft, and Professor Greenleaf and Mr Waters expressed support for the provision enabling the Privacy Commissioner to investigate acts and practices which occur outside of Australia.[113] The Australian Direct Marketing Association (ADMA) and Professor Greenleaf and Mr Waters supported

113 Google Australia Pty Limited, *Submission 16*, p. 6; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 4.

the extension of the protection under the extra-territoriality provision to cover the personal information of those who are not Australian citizens or permanent residents.[114]

11.108 Some submitters noted that paragraph 19(3)(g), does not clearly state where collection is deemed to have taken place.[115] The OPC provided comments in relation to the collection of information in the online context. The OPC pointed to the case where a person in Australia provided information to an overseas-based organisation. The OPC suggested that subsection 19(3) could clarify that:

> ...the Privacy Act applies to overseas acts or practices where the personal information is collected from or held in Australia. This may help to clarify that the Act applies where personal information is collected via the internet from an individual who is physically in Australia. There may also be alternative ways to clarify that personal information 'collected or held in Australia' includes such information collected over the internet.[116]

11.109 The OPC concluded that clarifying the scope of extra-territorial operation of the Privacy Act would enhance the Office's ability to apply the Act in these circumstances.[117]

11.110 Alternatively, two submitters suggested that, given that it is often difficult to ascertain the location of the user, the place of collection should be 'the place at which the information is collated and processed', therefore the provision should make it clear that:

> ...information is "collected" at the place (that is, in the jurisdiction) of the service provider collecting the information, not the place where the user is or may be presumed to be at the time that the information is collected.[118]

11.111 In its answers to questions on notice, the department commented that international internet services, such as entities engaged in online retail that sell to Australians, would be required to comply with the APPs so long as they fulfilled both branches of paragraph 19(3)(g). The department went on to state:

> It is likely that sub-paragraph 19(3)(g)(i) would capture businesses operating in Australia, but not businesses operating in foreign jurisdictions that happen to engage in commerce incidental to their primary purposes with customers in Australia.

---

114 Australian Direct Marketing Association, *Submission 27*, p. 8; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 4.

115 Google Australia Pty Limited, *Submission 16*, p. 6; Office of the Privacy Commissioner, *Submission 39*, pp 43-44; Law Council of Australia, *Submission 31*, p. 9.

116 Office of the Privacy Commissioner, *Submission 39*, p. 44.

117 Office of the Privacy Commissioner, *Submission 39*, p. 44.

118 Google Australia Pty Limited, *Submission 16*, p. 6; Law Council of Australia, *Submission 31*, p. 9.

> Collection takes place for the purpose of the Act when data is entered in Australia, regardless of the point of collation or processing. As such, the place of collection affects whether the Act applies, and once collection takes place s20, which sets out rules and responsibilities relating to the disclosure of personal information to an overseas recipient would apply with regard to acts or practices concerning the data collected.[119]

'Australian link'

11.112 Three submitters expressed concerns with the extension of the extra-territoriality provisions under section 19, as in practice this would mean that organisations with an Australian link, and every subsidiary or related body corporate of such organisations, will be subject to the APPs regardless of whether the information they are processing 'does not touch Australia and does not relate to the personal information of an individual in Australia.'[120] Each submitter suggested different options for limiting the application of the extra-territoriality provisions:

- the Law Council recommended that the Act should only extend to the acts and practices of an organisation under paragraph 19(3)(g) which relate to 'personal information that was collected or held in Australia by the organisation, or personal information about an Australian citizen or a permanent resident';[121]
- ADMA recommended that the extra-territoriality provisions be limited to apply only to companies with a presence in Australia;[122] and
- the FSC suggested that the APPs should not apply to 'information collected overseas by an entity that operates in Australia.'[123]

11.113 Further, the OPC raised concerns that the definition of 'Australian link' in the exposure draft differs slightly to the existing definition under the current legislation. The OPC noted that:

> As it refers to 'personal information' generally, it does not appear to require that 'the' specific item of personal information that is involved in a particular overseas act or practice was collected or held in Australia. This may unintentionally imply that, once an organisation collects or holds any personal information in Australia, an individual located overseas could complain under the Privacy Act about the organisation's acts or practices outside Australia, in relation to any personal information the organisation

119 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 30.

120 Law Council of Australia, *Submission 31*, pp 8–9. See also Australian Direct Marketing Association, *Submission 27*, p. 8; Financial Services Council, *Submission 34*, p. 3.

121 Law Council of Australia, *Submission 31*, pp 8–9.

122 Australian Direct Marketing Association, *Submission 27*, p. 8.

123 Financial Services Council, *Submission 34*, p. 3.

> holds about the individual (even if that information was never collected or held in Australia).[124]

11.114 The LIV noted that, under section 19 of the exposure draft, the APPs will apply to an organisation with an Australian link, however, under the current Privacy Act, the NPPs apply to an organisation if the act or practice relates to the personal information of an Australian citizen or permanent resident. The LIV expressed concern that the change of emphasis in the exposure draft may result in a reduction of protection for Australian citizens and permanent residents, particularly if they provide information to an agency which does not have an Australian link.[125]

11.115 The LCA also noted that while the current provisions stating that an act or practice required by an applicable law of a foreign country will not be taken as an interference with privacy will be replicated in the new Act, the existing provision, 'only applies to acts or practices required by foreign law (i.e. response to subpoena or other legal compulsion), not acts permitted in that jurisdiction.'[126]

11.116 The LCA expressed concern that:

> Disclosure under compulsion of Australian law is permitted, but not disclosure under compulsion of foreign law. This compounds the problem noted above, as (for example) a US office of an Australian corporation responding to US court process could find itself in jeopardy under Australian law (again, even if the data subject was not an Australian person or a person living in Australia). The Committee recommends that disclosures required under any law or legal process applicable to the organisation should be expressly permitted.[127]

11.117 The department responded to the LCA's concerns and stated:

> The exposure draft APPs is just one part of the process of amending the Privacy Act. As noted above, the Government intends for disclosure by organisations with an Australian link (as per s 19(3)) under foreign law to be a valid exemption from the operation of s 9(1).
>
> Provisions for the operation of foreign law in this way are currently enacted in section 13D of the Privacy Act. Since the policy intent behind these provisions has not changed, they have been replicated in the new APPs. Some minor issues relating to the definition of the law of a foreign country need to be resolved before this takes place, but these will be further revised in the reforms before they are brought before the Parliament.[128]

---

124 Office of the Privacy Commissioner, *Submission 39*, p. 43.

125 Law Institute of Victoria, *Submission 36*, p. 9.

126 Law Council of Australia, *Submission 31*, pp 8–9.

127 Law Council of Australia, *Submission 31*, pp 8–9.

128 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 30.

Conclusion

11.118 In relation to the concerns raised by the LCA, the committee notes that as stated in the Companion Guide, the policy achieved by subsection 6A(4) and section 13D of the *Privacy Act 1988*, will be replicated in the new Act ensuring that if an act or practice is required by an applicable law of a foreign country, it will not be taken as an interference with privacy.

11.119 The committee supports the concept of 'Australian link' as provided for in section 19. The committee notes that the policy intent that for a person to complain about the management about their personal information, that information must be held in Australia or collected in Australia. However, the committee has noted that there are concerns that this policy intent is not adequately expressed in proposed section 19. The committee therefore considers that further clarification on this matter is required.

Recommendation 19

11.120 The committee recommends that section 19, relating to the extraterritorial application of the Act, be reconsidered to provide clarity as to the policy intent of the provision.

Acts and practices of overseas recipients of personal information–section 20

11.121 Concerns were raised about the liability imposed on an Australian entity for the actions of an overseas entity, particularly, as under section 20 an entity is subject to strict liability even if it has taken all reasonable steps to ensure the overseas recipient complies with the APPs.[129] The AFC noted that section 20 only applies if information is disclosed to an overseas recipient under APP 8(1), but doesn't apply if the information is disclosed under APP 8(2). As a result, if information is disclosed to an overseas recipient under APP 8(2), it is the overseas recipient that remains liable, not the disclosing entity.[130]

11.122 The ABA considered this provision to be 'unreasonable' while Telstra noted that even if the entity takes all reasonable steps, there is still the possibility that the entity will not comply, which the Australian entity cannot prevent.[131] The Australian Association of National Advertisers noted that in some cases entities may have recourse through a contract but pointed to instances where, for example, an overseas recipient's computers are hacked. The AANA suggested that the provision is unfair if

129 Microsoft, *Submission 14*, p. 11; Australian Bankers' Association, *Submission 15*, p. 11; The Communications Council, *Submission 23*, p. 8; Deloitte Touche Tohmatsu, *Submission 28*, pp 1–2; Google Australia Pty Limited, *Submission 16*, p. 7; Law Council of Australia, *Submission 31*, p. 9.

130 Australian Finance Conference, *Submission 12*, pp 7–8.

131 Telstra, *Submission 19*, p. 5.

provision is not made for mitigating factors for example, personal information was obtained through hacking.[132]

11.123 The committee was provided with a range of suggestions to address the concerns raised:

- the LCA recommended where the disclosure complies with APP 8, the entity should not be liable for any acts done, or practices engaged in, by the overseas recipient in relation to that information;[133]
- the ABA suggested subsection 20(2) be qualified to limit application of the phrase 'for the purposes of this Act' to refer to the purposes of the compensation provisions of the Act, rather than the penalty provisions of the Act;[134]
- Telstra suggested that section 20 impose an obligation on an entity to 'use reasonable endeavours to ensure that the overseas recipient remedies any act or omission that would otherwise constitute a breach of the APPs';[135] and
- the AANA suggested that section 20 be amended to include exemptions to deal with mitigating factors.[136]

11.124 The department responded specifically to the AANA's comments and noted that unauthorised disclosure of personal information that has been lawfully transferred to a foreign entity via a breach of that foreign entity's data security would not, under the new Privacy Act, be a breach of section 20 as the breach and disclosure would not be an 'act or practice' of the foreign entity. The department added:

> The accountability of organisations which choose to transfer data across borders as provided for in s 20 is a necessary condition for the security of that data. Contracts in place between two entities involved in a cross-border transfer of data do not provide adequate protections for the individuals to whom the information pertains. As such, contracts are not an acceptable mitigating factor for the purposes of s 20.[137]

11.125 The LCA raised further concerns that the exposure draft does not specify a time period after which an entity is no longer liable for the acts or practices of an overseas recipient. In light of this, the LCA suggested that the liability imposed by section 20 be limited in time and aligned with other statutory limitation periods.[138]

---

132 Australian Association of National Advertisers, *Submission 21*, p. 8.

133 Law Council of Australia, *Submission 31*, p. 9.

134 Australian Bankers' Association, *Submission 15*, p. 11.

135 Telstra, *Submission 19*, p. 5.

136 Australian Association of National Advertisers, *Submission 21*, p. 8.

137 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 31.

138 Law Council of Australia, *Submission 31*, p. 10.

11.126 Further, the ABA voiced concern that an overseas data custodian, which has breached the APPs, may be able to limit its liability to the Australian data collector under Australia's proportionate liability laws.[139] The department commented on this point and noted that there is not currently any statutory limitation relating to the 'interference of privacy' that may occur under section 20. As the Act has not previously envisaged judicial enforcement (consistent with the principles-based nature of the Privacy Act), limitation periods have not been a relevant factor.

11.127 The department added that the ALRC has made a number of recommendations that the Australian Information Commissioner be given stronger enforcement powers, for example, the power to commence proceedings in the Federal Court or Federal Magistrates Court for enforcement orders and civil penalties. The department concluded:

> The Government has either accepted, or accepted in-principle, these recommendations, and will be developing draft amendments to address these issues. Relevant civil litigation rules that underpin this system, including statutory limitation periods, will be considered as part of the development of these amendments.[140]

11.128 Professor Greenleaf and Mr Waters questioned the ability of individuals to prove that a breach of the APPs has occurred in an overseas jurisdiction. They submitted that section 20 should be amended to provide that:

> ...a breach by an overseas recipient should be a rebuttable presumption if damage to the individual can reasonably be assumed to have resulted from the export.[141]

11.129 Telstra requested clarification regarding the possible application of APP 8 and section 20 to personal information which has been lawfully published. Telstra noted concern that if an overseas recipient accessed publicly available personal information, the entity which lawfully published the information might be held liable under section 20 for any inappropriate use of the information by an overseas recipient.[142]

11.130 The National Australia Bank (NAB), noted that it is unclear from the exposure draft how APP 8 and section 20 interact if the APPs apply to the overseas recipient, for example, if the overseas recipient is an entity with an Australian link. According to NAB, it appears that section 20 would not apply in these circumstances, however under APP 8(1) the entity would still have to undertake reasonable steps to ensure that the overseas recipient doesn't breach the APPs. Consequently NAB

---

139 Australian Bankers' Association, *Submission 15*, pp 11–12.

140 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 31.

141 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

142 Telstra Corporation Limited, *Submission 19*, p. 4.

submitted that section 20(1) and APP 8(1) should be made consistent to avoid confusion.[143]

11.131 The LIV raised a similar issue with regards to the interaction between APP 8 and section 19:

> APP 8(2)(a)(i) states that an entity is not bound to take reasonable steps to ensure that an overseas recipient of personal information collected in Australia does not breach the APPs if the entity reasonably believes that the overseas recipient is subject to a law or binding scheme that protects privacy in a 'substantially similar way'. Clause 19, however, intends to extend the application of the *Privacy Act 1988* (Cth) to an act done, or practice engaged in, outside Australia by an organisation that has an 'Australian link'. The LIV queries which provision prevails in circumstances where an overseas entity is captured by both APP 8 and cl 19.[144]

Conclusion

11.132 The committee received a range of comments in relation to section 20 in particular the application of the section in practice. The committee considers that further clarification is required, for example, through explanatory material to accompany the legislation.

Recommendation 20

11.133 The committee recommends that the Department of the Prime Minister and Cabinet develop explanatory material in relation to the application of the accountability provisions of section 20.

11.134 The committee also notes that the department has indicated that the Government has accepted the ALRC's recommendations in relation to stronger enforcement powers for the Australian Information Commissioner. The committee awaits with interest the exposure draft relating to the powers and function of the Information Commissioner.

143 National Australia Bank, *Submission 2*, p. 6.

144 Law Institute of Victoria, *Submission 36*, p. 7.

Chapter 12

Australian Privacy Principle 9–adoption, use or disclosure of government related identifiers

Introduction

12.1 Australian Privacy Principle 9 (APP 9) ensures organisations do not adopt government related identifiers as the identifier of an individual in their own system, as well as providing regulations on the use and disclosure of government related identifiers of an individual.

12.2 The Companion Guide states that APP 9 will ensure that identifiers issued by government agencies, for example Medicare numbers, are not used to facilitate unlawful data-matching by organisations. The Companion Guide explains that the intention of the principle is not to restrict organisations using government identifiers to verify the identity of an individual, but rather to prevent government identifiers from becoming general identifiers within organisations. The principle also aims to prevent government-issued identifiers from becoming 'de facto national identity numbers'.

12.3 APP 9 builds on the current identifiers privacy principle by incorporating State and Territory agency-issued identifiers, like drivers' licence numbers, within the scope of the regulations.[1]

Background

12.4 National Privacy Principle 7 (NPP 7) deals specifically with identifiers and ensures that private sector organisations neither adopt as the identifier of an individual within their own system, nor use or disclose, any identifiers of an individual assigned by a Commonwealth Government agency unless it is necessary to fulfil its obligations to the agency; it falls under a specified exception; or it is used by a prescribed organisation of a prescribed identifier in prescribed circumstances. There is no equivalent 'identifiers' principle in the Information Privacy Principles to regulate the use of government identifiers by agencies.[2]

12.5 Submitters to the Legal and Constitutional Affairs Committee inquiry into the Privacy Act in 2005 did not raise specific concerns regarding the identifiers principle, however issues relating to multi-purpose identity cards, like the Smart Card, were raised. Submitters noted that devices like the Smart Card could 'be used to establish a

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 13–14.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1024, p. 1027.

national identification scheme' and this should be avoided.[3] The Law Institute of Victoria (LIV) submitted that multi-purpose identifiers like the Smart Card and the Australia Card 'have the potential to become a technology of surveillance and control'.[4]

12.6 The ALRC review focussed on:

- whether a separate identifiers principle should be included in the model Unified Privacy Principles (UPPs);
- whether the identifier principle should extend to the adoption, use and disclosure of identifiers by agencies; and
- whether there should be changes to NPP 7 and the definition of the term 'identifiers'.

12.7 The ALRC came to the conclusion that there should be a separate 'identifiers' principle as it is not desirable that individuals be referred to by an agency-assigned identifier nor that data-matching be facilitated. Retention of a separate identifiers principle would also allow the Office of the Privacy Commissioner (OPC) to deal with issues relating to: 'the adoption of identifiers by organisations; the definition of the term; and the exceptions of the use and disclosure of identifiers by organisations'.[5]

12.8 The ALRC supported the retention of the exception to permit a prescribed organisation to adopt, use or disclose a prescribed identifier in prescribed circumstances as this 'ensures that the "Identifiers" principle does not operate inflexibly to prevent an organisation from carrying out activities that have a public benefit or are essential to the operations of the organisation'. The ALRC added that this exception should be set out in regulations. Further, the 'Identifiers' principle should require that the minister responsible for administering the Privacy Act needs to be satisfied that 'the derogation from the privacy protection in the 'Identifiers' principle is for the benefit of the individual concerned'.[6]

12.9 The ALRC review discussed the possibility of including public sector agencies within the identifiers principle. Some State and Territory laws regulate 'assignment, adoption, use and disclosure of identifiers by public sector bodies', with exceptions to ensure agencies carry out their functions or the individual agrees to the

---

3 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, p. 26.

4 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, p. 25.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1029.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1029.

agency using the identifier.[7] The ALRC also noted that there was support for the extension of NPP 7 to agencies and that this could 'promote regulatory consistency between agencies and organisations'.[8] However, many agencies argued that the inclusion of agencies in this principle would limit their capacity in carrying out efficient and effective service to their customers, and impede the operation of identity verification and fraud reduction programs and research. The ALRC agreed with the view put by agencies but went on to comment that it did not follow that 'the handling of identifiers by agencies should not be regulated'.

12.10 The ALRC considered the application of the principle to agencies subject to several agency-specific exemptions. However, the ALRC noted that this approach would be complicated and not consistent with the intended aim of making the principles more succinct. Rather, the ALRC supported an approach to 'regulate the assignment, collection, adoption, use and disclosure of identifiers by agencies on a case by case basis', similar to the approach taken to regulate Tax File Numbers.[9]

12.11 The ALRC review, like the Legal and Constitutional Affairs Committee inquiry, looked at the privacy risks associated with multi-purpose identifiers. The ALRC noted that if the Government were to introduce a multi-purpose identifier, it would most likely fall within the definitions of this principle. However, the ALRC recommended that before the introduction of any multi-purpose identifier, a Privacy Impact Assessment should be undertaken.[10]

12.12 In relation to the definition of 'Identifiers', the ALRC noted that NPP 7 does not describe what an identifier is. The OPC has published guidelines which expand on the definition in NPP 7. However, the ALRC considered that symbols and biometric information as identifiers of an individual should be included, not only numbers and letters. The ALRC agreed that an individual's name and ABN should continue to be excluded from the statutory definition of 'identifier'.[11]

12.13 Furthermore, the ALRC noted the difference between identification and verification or authentication and came to the view that the use of an identifier by an organisation for the sole purpose of verification 'is not inconsistent with the policy basis of the "Identifiers" principle. However, such a use or disclosure does not permit

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1030–31.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1031.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1034.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1057.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1035–40.

the organisation to adopt that identifier for its own purposes or use for a secondary purpose.[12]

12.14 The ALRC review also canvassed the issue of consent and whether this should be incorporated into the legislation to allow individuals to decide when their identifiers could be used or disclosed. The ALRC noted that including a consent clause would be convenient for organisations, however the ALRC and the OPC remarked that 'the privacy risks associated with identifiers are not always immediate' and the inclusion of a general consent exception would reduce an individual's protection under the identifiers principle.[13]

12.15 The review by the ALRC also looked at extending the identifiers principle to include State and Territory government issued identifiers and recommended their inclusion within a universal identifiers principle. The ALRC commented that 'the adoption, use and disclosure of these identifiers by organisations raises the same privacy concerns as those associated with other identifiers'.[14]

Government response

12.16 The Government accepted or accepted in principle all but one of the ALRC's recommendations. The Government noted that it was appropriate for public sector agencies to use and disclose identifiers to provide a public benefit, but at the same time protections must be in place to prevent the misuse of government issued identifiers, including State and territory government issued identifiers, by private sector organisations. In addition, the response noted the intent of section 7A of the *Privacy Act 1988* to have certain acts of certain agencies treated as the acts of organisations, so that when agencies are engaged in commercial activities they should comply with the Privacy Act in the same was as organisations. The Government response stated that a note to this effect should accompany the 'identifiers principle'.[15]

12.17 The Government agreed in principle with the exception recommended by the ALRC in relation to the adoption, use or disclosure of identifiers by organisations in prescribed circumstances as there are circumstances where this will provide a strong benefit to an individual. The Government plans to 'articulate the types of organisations

12 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 14, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 1042.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, pp 1046–47.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 1049.

15 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, p. 73.

that can interact with agency identifiers to provide services which are for the public benefit'.[16]

12.18 The Government accepted in principle that identifiers assigned by State and Territory agencies should be regulated by the principle and noted that the role played by these identifiers in the verification of an individual's identity. The Government indicated that it would ensure that the principle was drafted in such a way so as to not restrict the use of identifiers to verify identity 'where it is relevant and necessary to the organisation's functions'. The Government also indicted that it would encourage the OPC to develop guidance for organisations on when it would be appropriate to use identifiers for verification purposes. Furthermore, the response stated that before the introduction of any multi-purpose identifiers, the Government would ensure a Privacy Impact Assessment was carried out.[17]

12.19 The inclusion of biometric information within the definition of 'identifiers' was not accepted as the collection of such information 'will not result in the privacy risks that the "identifiers" principle is intended to address, such as the risk of an identifier becoming widely held and applied to facilitate data-matching or data-linking'. However, 'to future proof' the types of identifiers regulated by the principle, the Government indicated that the minister responsible for the Privacy Act 'will be able to determine what a government identifier is for the purposes of the Act'. Further this should be a legislative instrument.[18]

Issues

12.20 The general intention of APP 9 has been supported by several submitters to the inquiry.[19] Submitters also supported specific provisions of APP 9. Professor Greenleaf and Mr Waters, for example, commented that the inclusion of State and Territory Government-issued identifiers strengthens the restrictions on the private sector. This step was also supported by the OPC as it 'may facilitate further national consistency in personal information handling'.[20] However, the Australian Privacy Foundation argued that APP 9 would result in a weakening of the existing privacy principles.[21]

---

16 Australian Government, *Enhancing National Privacy Protection*, pp 73–74.

17 Australian Government, *Enhancing National Privacy Protection*, pp 75–76. The response also noted that the Government would review the current Tax File Number Guidelines.

18 Australian Government, *Enhancing National Privacy Protection*, p. 73 and p. 74.

19 Australian Institute of Credit Management, *Submission 8*, p. 4, Dr Colin Bennett, *Submission 11*, pp 3–4; Law Council of Australia, *Submission 31*, p. 7.

20 Professor G Greenleaf & Mr N Waters, *Submission 25*, p.15; Office of the Privacy Commissioner, *Submission 39*, p. 39.

21 Australian Privacy Foundation, *Submission 33*, p. 2.

Structure and terminology

12.21 Privacy NSW commented that APP 9 could be simplified by removing APP 9(2) and (3) (the use or disclosure of government identifiers and regulations about adoption, use or disclosure) from this principle and placing them into the Australian Privacy Rules. Privacy NSW also recommended that APP 9(4) and (5) (the explanations of the government related identifier and identifier) be included in the definition section of the legislation.[22]

12.22 The OPC again commented on the use of the term 'reasonably necessary' in the principles. 'Reasonably necessary' is used both in relation to the exceptions for verification of identity (APP 9(2)(a)) and fulfilling the obligation to an agency or State or Territory authority (APP 9(2)(b)). The OPC suggested that the term 'necessary' would be more appropriate as the entity proposing to use or disclose an identifier should be in a position to determine what is objectively necessary for the permitted purposes. In APP (2)(f), the exception related to law enforcement, again only 'necessary' should be used.[23] The OPC's comments were in line with its general view that the word 'reasonably' could qualify the meaning of necessary, 'lessening the protection provided in the current IPP and NPP requirements', adding that the word necessary on its own 'already implies an objective test'.[24]

12.23 The issues in relation to the use of the terms 'Australian law' and 'serious' were again raised by Qantas Airways Limited in relation to APP 9.[25] These matters are discussed in chapter 3.

Exclusion of agencies from APP 9

12.24 The major concern raised in submissions in relation to APP 9 is the continued exclusion of agencies from the coverage of this principle.[26] The Office of the Victorian Privacy Commissioner, for example, expressed concern that the principle does not provide the same level of protection against data-matching as the current Victorian Information Privacy Principle 7 (VIPP 7). The sharing of unique identifiers by the public sector, the Commission stated, 'is a very significant privacy risk' and excluding agencies from this principle does not 'represent the highest practicable level of privacy protection'.[27]

---

22 Australian Institute of Credit Management, *Submission 8*, p. 4; Privacy NSW, *Submission 29*, p. 6.

23 Office of the Privacy Commissioner, *Submission 39*, p. 39.

24 Office of the Privacy Commissioner, *Submission 39*, pp 6 and 18.

25 Qantas Airways Limited, *Submission 38*, pp 3–4.

26 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 8–9; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15; Health Services Commissioner, Victoria, *Submission 26*, p. 4.

27 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 8–9.

12.25 The inclusion of public sector agencies in this principle was also recommended by the Health Services Commissioner Victoria. The Health Services Commissioner argued that the restriction on adopting government related identifiers should also apply to health services such as public hospitals.[28] Professor Greenleaf and Mr Waters argued that 'the most significant abuse of government identifiers, data matching by government agencies,' should be regulated by APP 9 and suggested that the word 'organisation' should be omitted and replaced by 'entity'.[29]

12.26 In its response to this issue, the Department of the Prime Minister and Cabinet noted that the ALRC had considered arguments in favour of extending the application of the 'Identifier' principle to agencies. As discussed above, the ALRC noted that the inclusion of agencies could seriously impede activities conducted for a public benefit, including programs designed to reduce fraud and identity theft; service delivery; and research. It also noted that appropriate and important information sharing between agencies would be restricted. The ALRC noted that regulation of data-matching by agencies could be carried out either in separate sectoral legislation or guidance provided by the OPC. The department concluded 'as a result of these findings, the Government has not applied the requirements in APP 9 to agencies'.

12.27 The department also noted that 'in terms of existing protection in place to limit data-matching by agencies, some agencies are currently subject to data-matching requirements in legislation and in guidelines issued by the Privacy Commissioner'.[30]

12.28 A further matter raised in relation to agencies concerned the inclusion of the note after APP 9(1) and (2): 'An act or practice of an agency may be treated as an act or practice of an organisation'. The Health Services Commissioner, Victoria, commented that the note does not provide a clear explanation of how it expects agencies to be bound by APP 9(1) and (2). The OPC stated that this intention should be more explicit.[31] The committee notes that the Government response provides a brief explanation of this note to APP 9(1) and (2).[32]

Definition of identifiers

12.29 The NSW Department of Justice and Attorney General supported the ALRC's recommendation in relation to the definition of identifiers and commented that the inclusion of biometric information in the definition of identifiers was also recommended by the New South Wales Law Reform Commission's report on privacy principles. While noting the Government's reasoning for not including biometric data, the NSW Department of Justice and Attorney General argued that 'it is possible that,

28 Health Services Commissioner, Victoria, *Submission 26*, p. 4.

29 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15 and attachment, p. 17.

30 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 27.

31 Health Services Commissioner, Victoria, *Submission 26*, p. 4.

32 Australian Government, *Enhancing National Privacy Protection*, p. 73.

especially with advances in technology, biometric data may be used in the same way as a set of numbers in that it may be passed to various entities and linked to certain information'.[33]

Use or disclosure of government related identifiers

12.30 APP 9(2) provides for exceptions to the use or disclosure of an identifier, including an exception for the verification of identity of the affected individual. The Law Council of Australia (LCA) supported this exception and commented that this was important as it 'allows organisations to more easily comply with their obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*'. The LCA also noted that it will help organisations to 'use online customer verification tools for AML [Anti-Money Laundering] compliance purposes'.[34] The Australian Bankers' Association commented that this principle provides 'greater flexibility for use and disclosure [of government identifiers] in certain situations' than the current NPP 7.[35]

Regulations

12.31 The Australian Bankers' Association commented that APP 9(3) makes reference to compliance with regulations without clarifying what these regulations will be and when they will be introduced.[36] The committee notes that subsections 22(2) and (3) of the Exposure Draft provide for the making of regulations in relation to prescribe government-related identifiers if necessary. The ALRC noted that the power to make regulations provides the legislation with flexibility.

Conclusion

12.32 The committee has noted the comments by the OPC in relation to the use of the term 'reasonably necessary'. In the context of the identifiers principle, the committee considers that any exception should only be applied where it has been objectively determined that it is necessary for a permitted purpose. The committee therefore agrees with the OPC's suggestion that the term 'reasonably necessary' be replaced with 'necessary' in APP 9(2).

Recommendation 21

12.33 The committee recommends that the term 'reasonably necessary' be replaced with 'necessary' in APP 9(2)(a), (b) and (f).

12.34 The issue of biometric identifiers is of some concern to privacy advocates and submitters noted that the Government did not accept the ALRC's recommendation that

---

33 NSW Department of Justice and Attorney General, *Submission 42*, p. 9.

34 Law Council of Australia, *Submission 31*, p. 7.

35 Australian Bankers' Association, *Submission 15*, p. 14.

36 Australian Bankers' Association, *Submission 15*, p. 14.

the 'identifiers' principle apply to biometric information. The committee notes that the aim of APP 9 is to restrict the use to which government identifiers can be put. At the present time, while biometric information is used to establish the identity of individuals, it is not used as an 'identifier' in the same way as, for example, a Medicare or Tax File Number. The Government response states that the principle will be 'future proofed' as the minister responsible for the Privacy Act will be able to determine what a government identifier is for the purposes of the Act. The committee considers that this approach should adequately address any concerns with biometric information and emerging technologies in relation to this principle.

12.35 In relation to the exclusion of agencies from the operation of APP 9, the committee notes the ALRC's comments and the department's response to this issue. The committee notes that while the Australian Taxation Office, the Department of Veterans' Affairs and Centrelink are subject to *Data-matching Program (Assistance and Tax) Act 1990* in relation to specific matters, Commonwealth agencies generally are subject only to voluntary data-matching guidelines. Under the voluntary arrangement, agencies 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. The OPC will, where necessary, make recommendations in relation to the proposed protocols.

12.36 The ALRC considered that rather than inclusion of agencies in the obligations proposed by APP 9, a case-by-case approach should be taken similar to the approach taken to regulate Tax File Numbers (see paragraph 12.10 above). The ALRC also suggested that the OPC could exercise its function of researching and monitoring technology to review the adequacy of, and compliance with, the existing guidelines if it deemed this to be necessary. While the OPC did not comment on this matter in its submission to this inquiry, it submitted to the ALRC review that the existing voluntary data-matching guidelines should be reviewed and made mandatory.[37]

12.37 Further, the committee notes the proposed reforms under the Human Services Legislation Amendment Bill 2010 which will impact on the flow of personal information between Centrelink and Medicare. While there are significant benefits to government arising from data-matching, such activities pose risks to the privacy of individuals. The committee considers that data-matching should be authorised, transparent and conducted to appropriate standards. In addition, it may be the appropriate time to consider the directions for the future use of government identifiers. The committee therefore considers that a review of voluntary data-matching guidelines should be undertaken and that the outcome of that review should inform any further consideration of the extension of APP 9 to agencies.

37 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 443.

Recommendation 22

12.38 The committee recommends that the Office of the Australian Information Commissioner undertake a review of agency voluntary data-matching guidelines, including emerging issues with the use of government identifiers, and that the outcome inform further consideration of the extension of APP 9 to agencies.

Chapter 13

Australian Privacy Principle 10–quality of personal information

Introduction

13.1 Australian Privacy Principle 10 (APP 10) ensures that entities protect the quality of the personal information they collect, use and disclose. The Companion Guide notes that this principle will promote 'improved consistency of personal information handling practices by various entities' as well as reassure the public that entities will not use personal information that is 'based on misleading or erroneous information'.[1]

Background

13.2 The equivalent data quality principle is National Privacy Principle 3 (NPP 3), which requires private sector organisations to take reasonable steps to make sure that the personal information they collect, use or disclose is accurate, complete and up-to-date.

13.3 There is no equivalent Information Privacy Principle (IPP) which specifically covers data quality, however there are aspects of IPP 3 and IPP 8 which relate to data quality. IPP 3 which regulates the general solicitation of personal information, provides that where an agency collects personal information, it must:

> …take such steps (if any) as are in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected … the information collected is relevant to that purpose and is up-to-date and complete.

13.4 IPP 8 which requires record keepers to check the accuracy of personal information before it is used, provides that an agency:

> …who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up-to-date and complete.

13.5 There is currently no principle which regulates agencies at the time of disclosure of personal information.[2]

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 14.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 932.

13.6 The ALRC stated that 'ensuring the quality of personal information that is collected, used and disclosed, is recognised as a fundamental obligation of agencies and organisations under the Privacy Act'. These principles ensure that personal information handled by organisations and agencies is maintained at a high standard. In addition, data quality obligations 'will lead to greater consistency of, and increased public confidence in, the handling of personal information'[3]

13.7 The ALRC review focussed on:

- what changes were needed to improve the existing IPP and NPP data quality requirements into one Unified Privacy Principle; and
- the interaction of the data quality principle with the provisions of the other unified privacy principles proposed by the ALRC review.

13.8 The ALRC noted some inconsistencies between the current data quality requirements of the IPPs and NPPs. For example, IPP 8 imposes obligations on personal information that has been outsourced to another agency or organisation, as well as on an agency that holds information only on behalf of someone else. In addition, the IPPs include a provision that personal information collected, used or disclosed must be relevant.[4] The NPPs contain neither of these provisions.[5]

13.9 Furthermore, both IPP 3 and IPP 8 require that collection and usage occurs with regard to the 'purposes for which the information is collected', and 'having regard to the purpose for which the information is proposed to be used'. NPP 3 does not include such strict data quality provisions. The ALRC commented that these differences between the IPPs and the NPPs needed to be addressed when creating one universal principle applicable to both organisations and agencies.[6]

13.10 In regards to IPP 8, the ALRC remarked that this principle applies only to personal information in the agency's 'possession or control', not necessarily information being used by the agency. The ALRC was of the view that including this requirement in the data quality principle would create too high a compliance burden for agencies and organisations. This could also pose security risks for individuals as

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 931–932.

4 IPP 9 states that 'a record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.'

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 933–934.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 933–934.

third parties would have to contact individuals to ensure the personal information they possess is accurate, up-to-date, complete and relevant.[7]

13.11 To strengthen the current privacy principles, the ALRC stated that the revised data quality principle should include a clause emphasising that information collected, used or disclosed should be relevant to the purposes of the collection, use or disclosure of the information. The ALRC noted that this would complement the 'Collection' privacy principle as it sets out similar provisions in relation to data collection. The ALRC also stated that it would be logical to continue with a principle which limits the use and disclosure of personal information 'to that which is relevant to the purpose of that use or disclosure'.[8]

13.12 Furthermore, the ALRC argued that 'the fact that an agency or organisation has legitimately collected personal information for a permitted purpose should not mean that it is necessarily allowed to use or disclose *all* of that information'.[9]

13.13 There was comment in the ALRC review on whether to allow organisations and agencies to collect information which is not necessarily relevant until sometime after it has been collected. The ALRC argued that IPP 3 already provides that agencies have to collect information that is relevant to the purpose for which it is collected. Collecting information before it is clear that the information could be relevant would be in breach of the 'Collection' privacy principle and the ALRC advised it should also be a breach of the data quality principle.[10]

13.14 In addition, the ALRC commented that the inclusion of the requirement to ensure personal information collected, used or disclosed is relevant, 'would [not] impede the legitimate functions of agencies and organisations'.[11]

13.15 The ALRC noted that submitters to the Office of the Privacy Commissioner (OPC) 2005 review of the Private Sector Provisions of the Privacy Act had raised concerns regarding the obligations of the data quality principle. The Privacy Commissioner review stated that:

> Some organisations seem to consider that their obligations (under NPP 3) to keep personal information accurate, complete and up-to-date is an absolute obligation. Indeed, that it could be used to justify intruding upon an

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 936.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 937.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 937.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 937.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 937.

individual's privacy. However, obligations under the NPPs are not absolute.[12]

13.16 Submitters to the ALRC review remarked that it was not necessary to clarify that the obligations of the data quality principle were not absolute. Guidance on the issue has been published by OPC and the ALRC commented that this provided adequate clarification.[13]

Government Response

13.17 The Government accepted the ALRC's recommendations in relation to the data quality principle. The response noted that the requirements of the recommended unified principle would apply at the time of collection, use and disclosure. The Government noted that the inclusion of the phrase 'reasonable steps' 'reflect[ed] the intended proportional approach to compliance with this principle', including taking no steps if this was appropriate in the circumstances. Furthermore, the Government suggested the OPC publish guidance on the application of the data quality principle, including information on what constitutes reasonable steps.[14]

Issues

13.18 The data quality principle received broad support from many submitters to this inquiry.[15] The Office of the Victorian Privacy Commissioner remarked that it largely mirrors the existing NPP 3 and Victorian IPP 3.[16] The Health Services Commissioner of Victoria indicated that this principle is consistent with the equivalent Health Privacy Principle in the Health Services Act and, as such, was supported by the Commission. Further support was provided by Professor Greenleaf and Mr Waters, who recommended no changes to this principle and commented that it is a 'conventional principle of international standard'.[17]

13.19 The issues canvassed in submissions included the placement of APP 10 within the legislation, the concept of relevancy, and suggestions to expand the quality concept.

---

12 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), pp 267–268.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 939.

14 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, p. 61.

15 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 9; Australian Institute of Credit Management, *Submission 8*, p. 4; Professor G Greenleaf & Mr N Waters, *Submission 25*,p. 15.

16 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 9.

17 Health Services Commissioner of Victoria, *Submission 26*, p. 4; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15.

Structure

13.20 Privacy NSW recommended that if the privacy principles are to better reflect the information cycle, and how entities use personal information, APP 10 and APP 11 should be situated after the notification principle (APP 5) and before the use and disclosure principle (APP 6). Privacy NSW commented that the processes of ensuring quality and security of personal information should happen before decisions about use or disclosure of personal information occur.[18]

Relevance requirement

13.21 APP 10 contains two sections: APP 10(1) requires that entities take such steps (if any) as are reasonable in the circumstances to ensure that personal information collected is 'accurate, up-to-date and complete', while APP 10(2) requires that personal information used or disclosed is 'accurate, up-to-date, complete and relevant'.

13.22 Concerns about the exclusion of the concept of 'relevancy' to the collection of personal information (APP 10(1)) were raised by Dr Colin Barnett and the Law Institute of Victoria.[19] The Institute commented that 'entities should be obliged to collect, use and disclose only accurate, up-to-date, complete and relevant personal information'. This would be achieved by merging the two sections of APP 10 and would have the additional benefit of improve succinctness.[20]

13.23 The Department of the Prime Minister and Cabinet (the department) provided the committee with an explanation as to why 'relevant' was not included in proposed APP 10(1). The department stated that the proposed 'Collection' principle provides that personal information collected by an organisation should be 'reasonably necessary for, or directly related to, one or more of the entity's functions or activities'. The department submitted that 'including "relevant" in the collection-related data quality principle would have caused confusion with this overarching requirement in relation to collection'.[21]

13.24 The OPC commented on the relevance requirement in APP 10(2) and stated that it is not clear what is referred to by the term 'relevant'. The OPC went on to state that the 'relevance requirement should be linked to the purpose of use or disclosure' and that if the word 'relevant' is referring to the purpose of use or disclosure of information, this should be made more explicit in the wording of the principle. The OPC concluded that linking relevance to the purpose may give better effect to the policy intent of the ALRC's recommendation and the Government's Response to the recommendation which stated that:

---

18 Privacy NSW, *Submission 29*, p. 6.

19 Dr Colin Bennett, *Submission 11*, p. 4; Law Institute of Victoria, *Submission 36*, p. 7.

20 Dr Colin Bennett, *Submission 11*, p. 4; Law Institute of Victoria, *Submission 36*, p. 7.

21 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 28.

> Agencies and organisations should take reasonable steps to make certain that the personal information they collect, use or disclose is, with reference to the purposes of that collection, use or disclosure, accurate, complete, up-to-date and relevant. (emphasis added by the OPC).[22]

13.25 Privacy Law Consulting Australia raised a further matter in relation to the inclusion of the relevancy requirement in APP 10(2). It argued that entities adhering to APP 10(2) may be subject to privacy claims by individuals on new grounds, who could argue 'that a decision was made about them taking into account irrelevant information'. Privacy Law Consulting used the example of an insurance company refusing to provide an insurance policy to an individual, where the individual could claim that the insurer declined the service based on information not relevant to their application. Privacy Law Consulting submitted that these possible new grounds for privacy complaints will have 'significant implications for private sector organisations'. It argued that if this is not an intention of the principle, further consideration of the implications for organisations with the addition of the term 'relevant' should be made.[23]

13.26 In its answers to questions on notice, the department agreed that it would be possible under proposed APP 10(2) for individuals to make complaints about organisations if they did not take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the organisation uses or discloses is accurate, up-to-date, complete and relevant. The department noted that this is consistent with ALRC's recommendation that both organisations and agencies should have a data quality obligation with a 'relevance' element. The ALRC noted that it would complement the requirement in the 'Collection' principle that personal information collected by an organisation should be 'necessary for one or more of its functions or activities'.[24]

Information 'in control of an entity'

13.27 The Public Interest Advocacy Centre (PIAC) recommended that this principle should also apply to data already in control of an entity. PIAC argued that the burden for data quality in relation to sensitive information should be set higher than for other information and that the exclusion of information in control of an entity 'reduces the obligations that currently exist on agencies under IPP 8'. PIAC commented that the ALRC discussion on this matter did not deal sufficiently with the potential for data quality to be outside an entities' responsibility when data storage is outsourced. The ALRC was of the view that extending the principle to cover information in the control of an entity would impose an unjustified compliance burden on agencies and organisations (see paragraph 13.10). However, PIAC argued that while there may be an increased compliance burden on organisations, there would be no additional burden

---

22 Office of the Privacy Commissioner, *Submission 39*, p. 40.

23 Privacy Law Consulting, *Submission 24*, p. 8.

24 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 28.

on agencies and concluded that 'the adoption of UPPs should not see a reduction in protection in respect of personal information held by government'.[25]

Misleading information

13.28 The Office of the Information Commissioner Queensland suggested that the word 'misleading' be included in APP 10 as 'information may be correct, up-to-date and complete, but may still create a misleading impression in the mind of the reader'. The Commission remarked that there is a difference between inaccurate information and misleading information.[26]

Compliance burden

13.29 Coles Supermarkets criticised the requirements of APP 10 to continually ensure personal information is correct and up-to-date. Coles argued that this will place high administrative and cost burdens on entities, particularly large companies which use automated systems like Coles, where individuals contact the company to ensure the accuracy of their personal information.[27]

Conclusion

13.30 The committee has considered that issues raised in submissions, the department's response and views expressed by the ARLC in relation to data quality and makes the following comments. First, in relation to the expansion of the data quality obligation to 'information in the control of' an entity, the committee notes that the ALRC was of the view that this provision would place too high a burden on entities and could also pose a privacy risk for individuals.[28] The committee is in concurrence with this view.

13.31 Secondly, in relation to the suggestion that the obligation in APP 10 be expanded to include 'misleading' information, the committee notes that the Companion Guide states that 'having this principle reassures the public that the use of their personal information by entities is not based on misleading or erroneous personal information'.[29] The committee also notes that the ALRC did not make reference to 'misleading' information in relation to data quality except to the extent that it commented on the differences that would arise between the 'Access and Correction' principle (which contains the reference to 'misleading' information) and the 'Data Quality' principle (which does not contain the reference). The ALRC stated that it

---

25 Public Interest Advocacy Centre, *Submission 32*, p. 1 and Attachment p. 11.

26 Office of the Information Commissioner, *Submission 18*, p. 6.

27 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 4.

28 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 936.

29 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 14.

'considers this discrepancy to be appropriate, however, in light of the different context in which these principles operate'.[30]

13.32 In response to comments about the exclusion of the term 'misleading' in relation to the correction principle (APP 13) the department commented that it was not necessary to include the term 'misleading' in that principle as it was covered by the terms 'accurate' and 'relevant'. The committee therefore does not consider that the term 'misleading' needs to be included in APP 10.

13.33 Thirdly, the committee does not consider that the data quality provisions will increase the compliance burden for entities and notes that the requirements in APP 10 largely reflect those already contained in the National Privacy Principles.

13.34 Finally, in relation to comments about the term 'relevant', the committee notes that the obligations under APP 3 ensure that entities collect only personal information that is 'reasonably necessary for, or directly related to, one or more of the entity's functions or activities', that is, there is an implication of relevance to the entities functions or activities. Thus, the inclusion of the term 'relevant' in APP 10(1) is redundant. However, the committee notes the comments made by the Office of the Privacy Commissioner in relation to the need to clarify the use of the term 'relevant' in APP 10(2). The committee considers that if the word 'relevant' is referring to the purpose of use or disclosure of information, then this meaning is unclear and that the provision should be redrafted to clarify the matter.

Recommendation 23

13.35 The committee recommends that proposed APP 10(2), pertaining to the quality of personal information disclosed by an entity, be re-drafted to make clear the intended use of the term 'relevant'.

30 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 997.

Chapter 14

Australian Privacy Principle 11–security of personal information

Introduction

14.1 Australian Privacy Principle 11 (APP 11) protects personal information by imposing specific obligations on both agencies and organisations which hold that information. The principle also provides that entities take reasonable steps to destroy or de-identify the personal information once it is no longer needed. The Companion Guide noted that keeping personal information for only as long as 'reasonably necessary is an effective way of reducing the risk that it may be mishandled'. In addition, these obligations are in line with international best practice on privacy protection.[1]

Background

14.2 There are currently requirements within the National Privacy Principles (NPPs) and Information Privacy Principles (IPPs) which ensure agencies and organisations protect the personal information in their possession. NPP 4 requires organisations to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure as well as taking reasonable steps to destroy or de-identify information no longer needed.

14.3 IPP 4 requires that personal information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse. If the personal information is provided to a service provider, everything reasonably within the power of the agency is to be done to prevent unauthorised use or disclosure of information contained in the record.

14.4 The Australian Law Reform Commission (ALRC) noted the importance of a data security principle in privacy legislation, which is reflected by the provisions set out for both agencies and organisations to 'take reasonable steps to maintain the security of the personal information that they hold'. In addition, there are a number of international instruments relating to privacy which ensure the security of personal information.[2]

14.5 The ALRC review focussed on:

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, p. 14.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 941–942.

- how agencies and organisations should fulfil their data security obligations during the active life of records that contain personal information;
- disclosure of personal information to third parties; and
- the obligations of agencies and organisations to destroy or render non-identifiable personal information when it is no longer needed.

14.6 The ALRC recommended the data security principles be consolidated and simplified into a single principle. However, the ALRC commented that a consolidated principle would 'need to be sufficiently flexible to accommodate the differences' between the functions of the private sector and the public sector.[3]

14.7 The ALRC went on to comment that the criteria in the principle should ensure that personal information is 'protected from misuse and loss and from unauthorised access, modification or disclosure'. The ALRC explained that 'these criteria balance the role of the "Data Security" principle and those acts and practices that can be regulated more appropriately through other privacy principles'. Furthermore, the ALRC noted that some authorised access, use and disclosure can be improper and would not be regulated by the criteria above and are regulated elsewhere in the privacy principles by the data quality and use and disclosure principles.[4]

14.8 The ALRC also commented on the issue of personal information exchanged over the internet and whether it should be regulated by provisions in this principle. However, in keeping with the recommendation to keep the privacy principles technologically neutral, the ALRC considered that this step would not be necessary.[5]

14.9 In relation to the requirement on entities to take 'reasonable steps' to prevent the loss and misuse of personal information, the ALRC commented that 'implementing privacy-enhancing technologies will be one of the main ways through which agencies and organisations will comply with the requirement'. The ALRC acknowledged concerns by the Office of the Privacy Commissioner (OPC) on providing appropriate guidance on technological developments and recommended 'that the *Privacy Act* be amended to empower the Privacy Commissioner to establish expert panels at his or her discretion' to provide guidance on privacy-enhancing technologies.[6]

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 944.

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 949.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 949.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 950.

14.10 The ALRC considered the requirement of IPP 4 that provides that if an agency discloses personal information to a third party to carry out a service, the agency is required to take steps to prevent the unauthorised use and disclosure of this personal information by the third party involved. The ALRC did not recommend that such a requirement be included in the 'Data Security' principle. It noted that agencies remain regulated by section 95B of the Privacy Act[7] which provides that an 'agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles'. However, the ALRC commented that its position assumed implementation of a number of other recommendations including removal of the small business exemption from the Privacy Act and changes to the cross-border flow of data provisions. If these recommendations are implemented, the ALRC concluded that 'there will be few, if any, situations where a contracted party will not be under an obligation to comply with the Privacy Act.[8]

14.11 However, the ALRC remarked that if the above recommendations are not implemented 'then a requirement for organisations to take steps to protect information disclosed to a third party...will be an integral component of the *Privacy Act*'.[9]

14.12 In relation to the provision to de-identify personal information that is no longer needed, the ALRC recommended the phrase 'render de-identifiable' be used instead the NPP 4 wording of 'permanently de-identify'. The ALRC noted that this rephrasing would make it clearer that data destruction should include the prevention of re-identification of data in the future.[10]

14.13 Another concern raised during the ALRC review was the possible conflicts between the requirement to destroy data and the requirements of agencies to retain information. According to the ALRC, '[t]he data destruction requirement included in the "Data Security" principle must be worded so as to accommodate the various reasons why agencies and organisations may need to retain personal information'.[11] The ALRC noted that agencies are prohibited by the *Archives Act 1983* to destroy Commonwealth records without the permission of the National Archives, subject to certain exceptions. The ALRC noted however that the interaction between subsection 24(2) of the Archives Act and the destruction requirements of the Privacy Act were

---

7 'This section requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency', *Privacy Act 1988*, p. 187.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 954–55.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 955.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 958.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 963–965.

not clear. The ALRC recommended that 'agencies responsibilities under the *Archives Act* should take precedence over the data destruction requirement in the data security principle'.[12]

14.14 Another issue raised in the ALRC review was the concept of giving an individual the right to request an agency or organisation to destroy personal information that relates to that individual. The ALRC did not support this approach to data destruction, noting that it would be too rigid and would encourage destruction even when another method of dealing with the information may be more appropriate for example, rendering the information non-identifiable. The ALRC noted that rendering information non-identifiable still allows entities to evaluate the effectiveness of their projects, while not conflicting with the archives legislation obligations and ensuring that personal information is secure.[13]

14.15 In relation to guidance, the ALRC recommended that the OPC develop and publish guidance on matters including what constitutes 'reasonable steps' to prevent the misuse and loss of personal information by organisations and agencies; when it is appropriate to destroy or render non-identifiable personal information; the interaction between the data destruction requirements and legislative records retention requirements; and the manner in which personal information should be destroyed or rendered non-identifiable.[14]

Government Response

14.16 The Government responded positively to all the recommendations made by the ALRC in regards to the data security principle. The Government accepted that a data security principle should ensure the protection of personal information from loss and misuse, as well as the requirement to destroy and render non-identifiable information that is no longer needed. The Government noted that in relation to data destruction, the requirements on agencies to destroy or retain information as set out by the *Archives Act 1983* would not be affected.

14.17 The response supported the ALRC recommendations to have the OPC develop and publish guidelines on what constitutes 'reasonable steps' and the expected requirements on entities to destroy or render personal information non-identifiable.[15]

---

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 965.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 967.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 951; p. 970.

15 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, pp 62–63.

Issues

14.18 The issue of security of personal information was important to many of the submitters to this inquiry. Microsoft commented that 'security as an absolutely critical element of a privacy framework. Poor security makes privacy impossible.'[16] The Office of the Victorian Privacy Commission welcomed APP 11, remarking that it largely mirrors NPP 4 and Victorian IPP 4.[17] Similarly, the Australian Institute of Credit Management supported this principle and Yahoo!7 broadly agreed with its flexible approach.[18]

Structure

14.19 As discussed in the previous chapter, Privacy NSW suggested that APP 10 and APP 11 should be relocated within the legislation to better reflect the information cycle, that is, the quality principle and the security principle should be placed after the notification principle and before the use and disclosure principle.[19]

Protecting personal information

14.20 APP 11(1) provides that an entity must take such steps as are reasonable in the circumstance to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure. The Office of the Health Services Commissioner Victoria indicated support for APP 11(1) as did the Australian Bankers' Association (ABA) which welcomed the stronger emphasis on 'organisations to take all reasonable steps to ensure their systems and processes are secure'.[20] Other submitters commented on the 'reasonable steps' requirement, the protection of information accessed by contractors to agencies, and the inclusion of the term 'interference'.[21]

14.21 Microsoft submitted that 'getting security right is a bit more objective than some other aspects of privacy' and that the APPs could 'accommodate some more specific tests provided these did not affect cost effectiveness and were conducive to innovation'. In support of this view, Microsoft suggested 'a specified list of factors in the data security principle to help guide any determinations as to whether an organisation has taken "reasonable steps" to secure personal information it holds'.

---

16 Microsoft Australia, *Submission 14*, p. 12.

17 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 9.

18 Australian Institute of Credit Management, *Submission 8*, p. 4; Yahoo!7, *Submission 20*, p. 3.

19 Privacy NSW, *Submission 29*, p. 8.

20 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 4; Australian Bankers' Association, *Submission 15*, p. 14.

21 Australian Bankers' Association, *Submission 15*, p. 14; Telstra Corporation Ltd, *Submission 19*, p. 4; Australian Direct Marketing Association, *Submission 27*, p. 10; Privacy Law Consulting, *Submission 24*, p. 3 & p. 9; Office of the Health Services Commissioner Victoria, *Submission 26*, pp 4–5; Financial Services Council, *Submission 34*, pp. 3–4.

Microsoft has suggested this list be included in the legislation, or at least included with guidance issued by the Office of the Australian Information Commissioner once the legislation is in place.[22]

14.22 The NSW Department of Justice and Attorney General commented on the security requirements for information held by agencies which may be accessed by a contractor. It noted that, under section 95B of the Privacy Act, an agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles. However, APP 11 imposes no such requirement. While many organisations will be subject to APP 11, the small business exemption means that some organisations which may handle very sensitive personal information will not fall within the ambit of APP 11. The NSW Department of Justice and Attorney General recommended that consideration be given to replicating the requirement imposed on agencies by section 95B (and NSW legislation) 'in any model privacy laws if it is not to be provided for in the APPs'.[23]

14.23 The security of information in the hands of a contractor was also raised by the Privacy Interest Advocacy Centre (PIAC) in its submission to the ALRC review. PIAC stated that it was important to 'ensure that the data disclosed to third parties under contractual arrangements is maintained'.[24]

14.24 The National Association of Information Destruction (NAID-Australasia) suggested that APP 11 include a direction to entities that data protection policies and procedures be documented in writing. NAID-Australasia suggested that benefits would arise from such a requirement: having written policies and procedures is the only way to ensure that employees and vendors are given proper direction; and written policies and procedures is the only way an entity can demonstrate that it comprehends and takes its responsibilities to protect personal information seriously.[25]

Use of the term 'interference'

14.25 The ABA commented on the inclusion of the term 'interference' in APP 11(1)(a), and noted it is not present in the corresponding NPP. The ABA stated that it is not clear what the term intends to address, and sought specific guidance, with examples, on how it may occur and how 'interference' differs from the other listed factors of 'misuse', 'unauthorised access' and 'modification'.[26] The Australian Direct Marketing Association (ADMA) also noted the inclusion of the new term 'interference' in APP 11 and commented that the term is used broadly and without

22 Microsoft Australia, *Submission 14*, p. 12.

23 NSW Department of Justice and Attorney General, *Submission 42*, p. 10.

24 Privacy Interest Advocacy Centre, *Submission 32*, Attachment, p. 11.

25 National Association for Information Destruction, *Submission 6*, p. 3.

26 Australian Bankers' Association, *Submission 15*, p. 14.

proper definition. ADMA sought further clarification on 'how broadly the obligations that stem from this inclusion would be expected to apply'.[27]

14.26 Telstra expressed a similar view and went on to state that 'interference' could be viewed as 'unlawful interception' which requires further technological protections and 'degrees of encryption'. Telstra commented this could 'unfairly impose responsibility for external events or attacks' on organisations and lose the technologically neutral objective of the legislation. Telstra suggested the removal of the term 'interference'.[28]

14.27 The Department of the Prime Minister and Cabinet responded to these concerns and stated:

> The inclusion of 'interference' in APP 11 is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information (such as attacks on computer systems). It is correct that this element may require additional measures to be taken to protect against computer attacks etc, but the requirement is conditional on steps being 'reasonable in the circumstances'. Practical measures by entities to protect against interference of this nature are becoming more commonplace.
>
> The use of the term 'interference', which focuses on the activity rather than the means of the activity, ensures that the technologically neutral approach to the APPs is retained.[29]

Destruction of personal information

14.28 APP 11(2) provides for the destruction of records no longer required. NAID-Australasia supported information destruction as being a reasonable precaution for the security of personal information. However, it noted that the concept of destruction is often misunderstood, and gave the example of organisations relying on 'casual disposal or simple recycling as methods of destruction'. In order to clarify the meaning of destruction, NAID-Australasia recommended a definition of destruction within the definition section of the legislation. NAID-Australasia believed 'it is possible to define "destruction" while remaining technologically neutral, reasonable and non-descriptive'.[30]

14.29 The Office of the Health Services Commissioner Victoria commented that the provisions of APP 11(2) are not appropriate for the health industry as 'there may be a lapse of time in people re-presenting for treatment, or there may be medical conditions that are slow to progress'. The Commission recommended that a minimum retention

---

27 Australian Direct Marketing Association, *Submission 27*, p. 10.

28 Telstra Corporations Ltd, *Submission 19*, p. 4.

29 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 28.

30 National Association for Information Destruction, *Submission 6*, pp 3–4.

period for records be included in this principle, as is the case in Victoria, where the *Health Records Act* provides for a minimum retention period of seven years for health records. The Commission recommended that state and federal laws should continue to operate side by side, to ensure the seven year retention period is maintained.[31]

14.30 The Financial Services Council (FSC) requested further guidance on when it is appropriate to destroy or de-identify personal information, and the 'interaction between data destruction requirements and legislative record retention requirements'. The Council stated that retaining records for seven to ten years from the last date of interaction with the client is standard practice in the financial services industry and recommended that the requirement to destroy or de-identify personal information 'commence after other legal requirements for record retention timeframes have been met'.[32]

14.31 Yahoo!7 suggested that the provisions for the retention of personal information rely on 'legitimate business purposes' rather than the purposes of APP 10 and APP 11.[33]

14.32 Google Australia stated that subsection APP (2)(c) should be amended to allow for compliance with foreign laws. Google noted that they conduct business worldwide and are required to comply with both Australian Privacy Laws and Foreign Privacy Laws.[34] (The committee has commented on this matter in chapter 3, see paragraphs 3.77–78.)

14.33 Privacy Law Consulting Australia raised concerns about this privacy principle conflicting with section 24 of the Archives Act and creating a circular process of interaction between the provisions of the two Acts. The Consultancy suggested including information within APP 11 to explain its interaction with section 24 of the Archives Act.[35] Similar points were raised by the ALRC (see para 14.18). The Government response stated that the ALRC's recommendation in relation to destruction or de-identifying information 'does not affect the operation of the *Archives Act 1983* on how agencies retain personal information'.[36]

Conclusions

14.34 The issue raised by the NSW Department of Justice and Attorney General and the Privacy Interest Advocacy Centre concerned the protection of information held by agencies which may be accessed by third parties, for example, contractors. The

---

31 Office of the Health Services Commissioner Victoria, *Submission 26*, pp 4–5.

32 Financial Services Council, *Submission 34*, pp 3–4.

33 Yahoo!7, *Submission 20*, p. 3.

34 Google Australia, *Submission 16*, pp 6–7.

35 Privacy Law Consulting, *Submission 24*, pp 3, 9.

36 Australian Government, *Enhancing National Privacy Protection*, p. 63.

committee notes that the ALRC did not recommend such a requirement. Further, the ALRC commented that agencies remain subject to section 95B of the Privacy Act which provides that an agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles. The Government has not indicated that a provision similar to section 95B will not be retained in the new Act. However, the committee will consider this matter further when the relevant exposure draft is provided.

14.35 In relation to comments concerning the inclusion of the term 'interference' in APP 11(1)(a), in particular that its meaning is unclear, the committee notes that the department has indicated that 'interference' is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information. The department provided the example of 'interference' through an attack on a computer system. The committee considers that this is an essential protection for personal information and supports the inclusion of the term 'interference'. However, the committee believes compliance with this principle would be improved if the term 'interference' was defined or a note was included to explain its meaning.

Recommendation 24

14.36 The committee recommends that a definition of the term 'interference' used in proposed APP 11(1)(a), pertaining the security of personal information, be provided or a note included in the legislation to explain its meaning in this context.

14.37 The committee considers that the destruction of personal information no longer required is an important matter. The committee notes the concerns raised by NAID-Australasia that destruction of information is often misunderstood and approached in a less than appropriate manner. The committee considers that it will be important that guidance is provided in relation to what constitutes 'destruction' in relation to personal information. The committee also notes that submitters called for guidance on range of other matters and that the need for guidance from the Office of the Australian Information Commission was recommended by the ALRC and accepted by the Government.

Recommendation 25

14.38 The committee recommends that the Australian Information Commissioner provide guidance on the meaning of 'destruction' in relation to personal information no longer required and the appropriate methods of destruction of that information.

14.39 Submitters did not comment on the use of the term 'to ensure that the information is no longer personal information' in relation to APP 11 however, comments were made in relation to APP 4, see chapter 7.

Chapter 15

Australian Privacy Principle 12–access to personal information

Introduction

15.1 Australian Privacy Principle 12 (APP 12) ensures that a person can access their own personal information held by an entity other than when exceptions to granting access apply. APP 12 also provides for how entities are to deal with requests for access, access charges and how entities should respond to an individual when access is refused.[1]

15.2 It is noted in the Companion Guide that APP 12 is aimed at ensuring that individuals have access to the information that entities hold about them and that there is opportunity to correct inaccurate, irrelevant and out-of-date information. There are a limited number of circumstances which an entity may refuse to give individuals access to their own personal information. However, in these circumstances entities have an obligation to provide as much access as is possible in the circumstances to meet the needs of the individual and the entity.[2]

Background

15.3 APP 12, together with APP 13 (correction of personal information), replaces existing Information Privacy Principle 6 (IPP 6), and National Privacy Principle 6 (NPP 6). Currently, agencies must provide access to personal information under IPP 6 except to the extent that an agency is required or authorised to refuse assess under any law of the Commonwealth that provides for access by persons to documents. IPP 6 provides individuals with the same rights as the *Freedom of Information Act 1982* (FOI Act).[3]

15.4 NPP 6 provides that generally, an organisation that holds personal information must provide the individual with access to the information. A list of situations where access can be denied or limited is also provided in NPP 6. Where an organisation is not required to give access, it must consider whether the needs of both parties can be met through the use of a mutually agreed intermediary. NPP 6 also provides that an organisation must take reasonable steps to correct personal information that it holds, if the individual to whom the information relates, is able to establish that it is not accurate, complete and up-to-date. Where there is a disagreement about the accuracy

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 14.

2 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 14.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 973.

of the information, the organisation, if requested by the individual, is to take reasonable steps to associate with the information a statement claiming the information is not accurate, complete or up-to-date.[4]

15.5 The Australian Law Reform Commission's (ALRC) review of the access provisions of the Privacy Act considered both the structure of the principle and how the access provisions should be framed, particularly to allow for a unified principle for agencies and organisations.

15.6 The ALRC came to the view that it was possible for the 'Access and Correction' principle to apply equally to both agencies and individuals and recommended this change.[5] The ALRC also compared the structure of NPP 6, which contains both general, high-level provisions and more detailed, relatively prescriptive provisions, and IPP 6, which contains more general rules.

15.7 The ALRC concluded, as it had in its earlier report, *Review of Australian Privacy Law* (DP72), that NPP 6 should form the basis of the unified 'Access and Correction' principle.[6] The ALRC pointed to the following matters for this conclusion:

- the NPP structure is preferable because the relevant and applicable legislation is not fragmented among several separate Acts, as is the case under the IPP structure. For example, the IPPs do not contain procedural provisions for agencies to follow when processing applications for access. Instead, the IPPs rely on 'administrative machinery' contained within the FOI Act;[7]
- the NPP structure is comparatively simpler to navigate, to understand and to use;
- if the IPP structure prevailed in the development of the new APP regime, transferring the administrative machinery of the FOI Act into the APP legislation would require the Privacy Principles to be redrafted so that their 'provisions...operate as conventional statutory provisions, as distinct from principles'. Such a fundamental change in the character of regulation would be

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 974; see also Australian Law Reform Commission, *Review of Australian Privacy Law (DP72)*, p. 171.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 977.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 976; Australian Law Reform Commission, *Review of Australian Privacy Law (DP72)*, pp 89–100.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 975.

a reorienting from principles-based regulation to rules-based regulation; a change which the ALRC did not support;[8] and

- a radical restructuring of the regulatory regime for organisations would impose 'a greater compliance burden, particularly on organisations that would have to update their privacy protection regimes'.[9]

15.8 In considering how the access provisions should be framed, the ALRC distinguished between the right to obtain access in IPP 6 and the obligation on organisations to provide access in NPP 6. The ALRC concluded that the provision should be expressed as an obligation on an agency, rather than an entitlement of an individual. A further point of difference between IPP 6 and NPP 7 is that the former applies to personal information that is in an agency's 'possession or control' while the latter applies to personal information 'held by an organisation'. The ALRC concluded that the word 'held' should be retained in the 'Access and Correction' principle with 'held' including those documents over which an entity has 'constructive possession'.[10]

15.9 While both the IPPs and NPPs place obligations on agencies and organisations to provide individuals with access to personal information that they hold about the person, the exceptions for this obligation differ. The ALRC's view was that exceptions to the 'Access and Correction' principle should be consistent with the FOI Act and the *Archives Act 1983* (Archives Act) as individuals should not be able to compel access under the Privacy Act that would otherwise be exempt under the FOI Act or the Archives Act.[11] In relation to the content of the exceptions, the ALRC made the following comments:

- *threat to life or health*: an individual should not be able to obtain personal information that an organisation holds about him or her if providing access would pose a serious threat to the life or health of an individual; and
- *other exceptions to access*: the existing exceptions in NPP 6 should be included in the 'Access and Correction' principle.[12]

15.10 The ALRC also considered the use of third party intermediaries where access to information has been lawfully denied as currently provided for in NPP 6.3 in certain cases. The ALRC commented that it was important that there is a provision

---

8 See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, Chapter 4, for a detailed discussion of principles-based and rules-based regulation.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 976.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 978–79.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 982.

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 986–87.

requiring an agency or organisation to take reasonable steps to provide an individual with as much personal information as possible, in circumstances where access to the information legitimately can be refused and stated 'such a provision allows for a more flexible, nuanced approach to requests for access where direct access is not appropriate'.[13]

15.11 However, the ALRC did not support the present requirement in NPP 6.3 that an organisation must 'consider' the use of a mutually agreed intermediary. The ALRC saw the potential for abuse of this provision in that organisations could comply with the requirement by briefly contemplating, and then immediately rejecting, such a course of action. In addition, the ALRC considered that the intermediary requirement proposed in DP72, that an organisation 'reach an appropriate compromise' with an individual seeking access to personal information, was ambiguous and that there was a need for a more clearly stated requirement. The ALRC therefore recommended the 'Access and Correction' principle should provide that where an entity is not required to provide an individual with access to his or her personal information, the entity 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.[14]

15.12 The ALRC also considered the procedural requirements for access. While NPP 6 contains procedural requirements for organisations including limits on the charges that they can levy for providing an individual with access, the IPPs do not. The ALRC concluded that procedures imposed on organisations under the 'Access and Correction' principle should also apply to agencies. In addition, the ALRC commented specifically about the following procedural matters:

- *fees:* fees charged by an organisation for providing access to information, as contained in NPP 6.4, should be continued. However, it was not recommended that these provisions be extended to agencies;
- *timeliness of response:* both agencies and organisations should respond to requests for access within a reasonable time;
- *manner of providing access:* the 'Access and Correction' principle should require agencies to take reasonable steps to provide access in the manner requested by the individual; and
- *level of detail of the provisions:* the ALRC did not support binding schedules or frameworks for the provisions as there would be practical difficulties with

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 991.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 993.

such an approach and the use of high-level principles was consistent with its broader approach to privacy regulation.[15]

15.13 In relation to reasons for a decision to deny access to personal information, the ALRC concluded that it is an important element of procedural fairness for the individual to be provided with the reason for the adverse decision. However, there may be situations where providing the reason for the decision could undermine the reason the agency or organisation has denied the access and in these situations the ALRC did not support the provision of reasons. The ALRC also recommended that the individual should be provided with the avenues for complaint.[16]

15.14 The ALRC also recommended that the Office of the Privacy Commissioner develop and publish guidelines to ensure that agencies and organisations are provided with clear guidance on how the changes should be applied.[17]

Government response

15.15 The Government accepted, accepted with amendment, or accepted in principle all of the ALRC's recommendations in relation to access and correction. In accepting that a unified 'Access and Correction' principle should apply to both agencies and organisations, the Government noted the implications for the interaction between the Privacy Act and the FOI Act and stated:

- as part of proposed reforms to the FOI Act, it was announced that the Privacy Act would be amended to enact an enforceable right of access to, and correction of, an individual's own personal information, rather than maintaining the right through the FOI Act;
- that it would be necessary to recognise the additional responsibilities of Government in relation to the disclosure of some categories of information and documents;
- that amendments will make it clear that the right to access and correct information held by agencies will be provided by the Privacy Act rather than the FOI Act although the right to access some personal information will remain under the FOI Act; and
- processes around reviews of agency access and correction decisions under the Privacy Act will be aligned as closely as possible with reviews under the FOI Act.[18]

---

15 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1012–14.

16 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1017.

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1018.

15.16 The Government accepted with amendment recommendation 29–3 which provided that where an organisation holds personal information about an individual, it is not required to provide access to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of an individual. The Government response indicated that to ensure consistency, a 'serious threat' should refer to 'life, health or safety'.

15.17 The Government also accepted with amendment recommendation 29–7 which contains the obligation to respond to an access request within a reasonable time and to provide access in a manner requested by the individual, where reasonable and practicable. The Government commented that the ALRC was silent on the issue of entities charging for access, however, the Government agreed that where an organisation imposes a charge for access, is should not be excessive and must not apply to lodging a request for access.

15.18 The Government accepted with amendment the recommendation relating to denial of a request for access. The Government commented that the principle should explicitly provide for situations where providing reasons would undermine the reason for denying the request for access. Further, the principle should recognise that, where reasons can be provided for an adverse decision, the reasons should specify any relevant exceptions, requirements or authorisations relied upon in making the decision.[19]

Issues

15.19 The Australian Institute of Credit Management supported APP 12.[20] However, other submitters raised several issues in relation to APP 12 including the enforceable right of access; the range of exceptions; and time limits for processing applications.

Enforceable right of access

15.20 The Victorian Privacy Commissioner commented that the Government had announced, as part of the reform of the FOI Act, that the Privacy Act would be amended to provide for an enforceable right of access to an individual's own personal information. While noting the importance of the right of an individual to access and

18 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice,* October 2009, pp 62–65.

19 Australian Government, *Enhancing National Privacy Protection First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, p. 71.

20 Australian Institute of Credit Management, *Submission 8*, p. 4.

correct their personal information, the Victorian Privacy Commissioner stated that 'the language of APP 12 does not currently reflect this'.[21]

15.21 The Companion Guide notes that an enforceable right of access to (and correction of) an individual's own personal information 'does not appear on the face of Australian Privacy Principles 12 and 13'. It was noted that this is because there are a large number of technical issues in relation to the way that the Privacy Act and FOI Act will interact 'that have not yet been fully resolved'. The Companion Guide also stated that the APPs set up some of the technical infrastructure that will link into other provisions of the Privacy Act and provide the means for merits review as well as provision for additional notice requirements to be prescribed by the regulations. The Companion Guide concluded:

> This ensures that there is basic content for notification of decision contained in the legislation, but with capacity to prescribe additional requirements so that the provisions of the Privacy Act are consistent with those in the *Freedom of Information Act 1982*.[22]

Structure and terminology

15.22 Submitters were concerned by loose and overly complex language and the repetition of clauses in APP 12. The Office of the Privacy Commissioner (OPC) for example, suggested the removal of the apparently redundant section APP 12(5)(a) as the following paragraph refers to refusing access under relevant provision. This would result in a simplified structure for APP 12(5).[23] Privacy NSW noted that the exceptions in APP 12(3) were 'dense and complex'.[24]

15.23 The Department of the Prime Minister and Cabinet responded:

> This single principle is more lengthy and prescriptive than other APPs (eg collection, use and disclosure) for a number of reasons. First, it is intended to consolidate the existing access and correction obligations in IPPs 6 and 7 for agencies and NPP 6 for organisations. It is also intended to clarify the existing overlap between the Privacy Act and the FOI Act, with the provisions and administrative machinery under the FOI Act being, in practice, the primary means for dealing with access and correction requests from individuals. In addition, it was also necessary to outline the separate and broader range of exceptions to access for organisations. Finally, it was necessary to set out the process once a request for access is received.[25]

---

21 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 10.

22 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 18–19.

23 Office of the Privacy Commissioner, *Submission 39*, p. 41.

24 Privacy NSW, *Submission 29*, p. 5.

25 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 29.

Conclusion

15.24 The committee has provided comments concerning the issue of complexity of the APPs in chapter 3 of this report. As noted in that chapter, the committee considers that some fine tuning of the APPs would improve clarity and simplicity particularly through the use of more concise language and elimination of redundant clauses.

Exceptions

15.25 APP 12(2) contains exceptions to access if the personal information is held by an agency and APP 12(3) contains exceptions to access if the personal information is held by an organisation. Professor Greenleaf and Mr Waters argued that proposed APP 12(2) and 12(3) expand on the current grounds for refusing access, and includes new exceptions, 'without any convincing justification'.[26]

15.26 Other submitters raised concerns with the exceptions in relation to organisations. The Law Institute of Victoria (LIV) commented on two of these exceptions. The first, APP (3)(b), provides an exception where giving access would have an unreasonable impact on the privacy of other individuals. The LIV considered that this exception may be difficult to apply where information about an individual is an opinion, as this is potentially the personal information not only of the person who is the subject of the opinion, but of the person who holds that opinion. In relation to the exception contained in APP 12(3)(e)–where giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations–the LIV raised concern about the broad nature of the provision. The LIV commented that there appeared to be no limitations or parameters about what phase of negotiations the parties are in, such as whether the negotiations need to be already commenced, or at least reasonably anticipated, before this clause becomes operative.[27]

15.27 Dr Colin Bennett criticised the inclusion of the 'frivolous or vexatious' exception (APP 12(3)(c)) as 'the right to access ones personal information is a human right, regardless of motive' and submitted that the 'frivolous or vexatious' exception under APP 12(3)(c) is open to abuse 'especially where individuals might be in conflict with a particular organization over a particular matter, and reasonably want to know everything the organization holds on them'. Dr Bennett concluded:

> At the very least, the provision should state that the organization should be obliged to report and account for the use of this discretion.[28]

15.28 The Office of the Health Services Commissioner (OHSC) also raised concerns in relation to APP 12(3)(c) and stated that this was not an appropriate exception in relation to health information because 'a person has a right to access their health

---

26 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 16.

27 Law Institute of Victoria, *Submission 36*, p. 8.

28 Dr Colin Bennett, *Submission 11*, p. 5.

information, even if the contents are brief'. The OHSC commented further that an individual does not require a reason to access their health information, and such an exception is likely to lead to organisations refusing access 'without good reason'. The OHSC believed that the other exceptions available to organisations under APP 12(3) provide sufficient protection for organisations to refuse access without APP 12(3)(c) being necessary also.[29]

15.29 Google's submission discussed the international dimension of Google's business and operations. Google noted that entities operating in Australia are subject not only to Australian regulation but also foreign regulation, such as in the case of a business based in one country with activities in another country being required to comply with regulations of both countries. Google noted that due to these requirements to comply with foreign laws, the reference to 'Australian law' in APP 12(3)(g) should be amended so that the need to comply with foreign laws also constitutes an exception under APP 12(3).[30]

15.30 The exception related to information which is generated in connection with a commercially sensitive decision-making process (APP 12(3)(j)), was compared to the current provisions provided by its equivalent, NPP 6.2. The OPC noted that in NPP 6.2, an organisation 'may give the individual an explanation for the commercially sensitive decision rather than direct access to the information'. The OPC commented that although it may be intended that the existing right is given effect by way of APP 12(5) and APP 12(9), it is unclear and should be clarified so that the right to be given reasons for a decision is preserved.[31]

Dealing with requests for access

15.31 The OHSC raised concerns with APP 12(4)(b) which requires that the entity must give access in the manner requested by the individual, if it is reasonable and practicable to do so. The OHSC considered that such an exception should not apply in relation to personal health information. It argued that as most people seek access in the form of a copy, the exception may permit organisations to offer personal inspections of records rather than providing access in the manner requested. This alternative would be more expensive for individuals, as supervision by a staff member would be required. The OHSC concluded that such an outcome 'would be unsatisfactory and contrary to the principle of patient autonomy that applies in a health setting'.[32]

---

29 Office of the Health Services Commissioner, *Submission 26,* p. 5.

30 Google Australia & New Zealand, *Submission 16*, p. 8.

31 Office of the Privacy Commissioner, *Submission 39*, p. 41.

32 Office of the Health Services Commissioner, *Submission 26,* p. 5.

15.32 The Public Interest Advocacy Centre (PIAC) commented on the inclusion of the term 'where reasonable and practicable'. This matter was first raised during the ALRC consultation process. PIAC commented:

> ...the limit on the obligation in UPP 9.5 created by the inclusion of the term 'where reasonable and practicable' could very easily result in unlawfully discriminatory limits on access both in terms of format of information and in terms of any requirement to travel to a particular location to access that information.[33]

Time limits for responses

15.33 APP 12 requires agencies to respond to requests for access within 30 days (APP 12(4)(a)(i)) and organisations to respond to requests 'within a reasonable period' (APP 12(4)(a)(ii)). This preserves the current arrangements in the Privacy Act.

15.34 Westpac was the only submitter to voice a preference for not setting clear timeframes, instead supporting the proposed regime:

> Westpac notes and supports the approach of "reasonableness" when determining a timeframe for a response to an individual, in preference to setting a specified period in which to comply. In developing guidance for industry regarding reasonable response times, we recommend the OPC engage closely with industry to develop flexible and appropriate guidance.[34]

15.35 Other submitters called for greater clarity as to the timeframe in which an organisation is to respond to a request for access. The OPC submitted that the differing standards under APP 12(4) between agencies and organisations 'may unintentionally imply that a reasonable period for organisations to provide access may be longer than 30 days'.[35] The OPC noted that guidance produced by the Office suggested access should be granted within 14 days, if granting access is straight forward, or within 30 days, if access is more complicated. The OPC suggested that a note under APP 12(4)(a) could clarify that a reasonable period would not usually be longer than 30 days.[36]

15.36 The OHSC commented that a fixed timeframe was preferable in the health sector and would remove uncertainty. The OHSC also noted the Victorian Health Records Act contains a requirement that organisations respond to a request for access within 45 days.[37]

---

33 Public Interest Advocacy Centre, *Submission 32,* Attachment A, p. 12.

34 Westpac, *Submission 13,* p. 3.

35 Office of the Privacy Commissioner, *Submission 39,* pp 40-41.

36 Office of the Privacy Commissioner, *Submission 39,* p. 9.

37 Office of the Health Services Commissioner, *Submission 26,* p. 5.

Other means of access

15.37 APP 12(5) provides that where an entity refuses access, or refuses to give access in the manner requested, the entity must take such steps as are reasonable to give access in a way that meets the needs of the entity and the individual. The Australian Bankers' Association commented that this obligation 'should provide, in the majority of cases, a workable outcome and avoid escalation of any disagreement'.[38] However, Abacus Australian Mutuals questioned the need for this additional obligation on an entity 'particularly given the fact that the listed exceptions to access are well founded'.[39]

15.38 The OPC submitted that by referring to the needs of the entity, the emphasis is shifted away from the individual and suggested that the phrase 'the needs of the entity' should be removed. The OPC concluded that reasonable steps requirement allows sufficient flexibility to meet an entity's needs and obligations under APP 12.[40]

Access charges

15.39 APP 12(8) allows for entities to charge for access so long as the charge is not excessive and does not apply to the making of the request for access. The LIV commented that an entity is not necessarily precluded from charging unreasonable amounts or profiteering. The LIV suggested that 'excessive' be replaced with 'reasonably necessary to recoup the costs incurred by the entity'.[41]

Conclusion

15.40 The committee considers that it is important to ensure that balance exists in the privacy regime between the interests of individuals and entities. Conversely, there should not be an excessive number of exceptions which may inhibit an individual's right to access personal information. In discussion of APP 12, the Companion Guide states:

> There are a limited number of circumstances in which an entity may refuse to give individuals access to their own personal information.[42]

15.41 However, submitters raised concern that some of these 'limited' exceptions are broad, open-ended, and may be open to abuse. The committee considers that this may not only give rise to confusion, but also the potential for unwarranted denials of access to personal information. In particular, the committee is mindful of the comments of the Law Institute of Victoria that the exception in relation to negotiations

---

38 Australian Bankers' Association, *Submission 15*, p. 15.

39 Abacus Australian Mutuals, *Submission 7*, pp 2–3.

40 Office of the Privacy Commissioner, *Submission 39*, p. 40.

41 Law Institute of Victoria, *Submission 36*, p. 8.

42 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 14.

(APP 12(3)(e)) is too broad as well as the comments in relation to the 'frivolous or vexatious' exception (APP 12(3)(c)) particularly its application in the health sector. The committee considers that the negotiations exception in APP 12(3)(e) could be improved by provided greater clarity as to when this exception may be invoked.

15.42 The OPC also commented that the exception concerning commercially sensitive decision making processes (APP 12(3)(j)) does not contain the currently provided for option of an organisation providing an explanation rather than direct access. While the ALRC noted that concerns were raised by privacy advocates that the option of an explanation instead of direct access could be used inappropriately to deny direct access, the OPC considered that individuals should retain the same rights as are currently contained in the Privacy Act. The committee agrees with this approach and considers that further consideration should be given to this exception.

Recommendation 26

15.43 The committee recommends that, in relation to the proposed exceptions provided for in APP 12(3):

- **the Australian Information Commissioner provide guidance in relation to the application of the 'frivolous and vexatious' exception (APP 12(3)(c));**
- **clarity be provided as to the stage at which the negotiations exception in APP 12(3)(e) may be invoked; and**
- **further consideration be given to the exception in APP 12(3)(j) in relation to commercially sensitive decisions to ensure that the rights currently provided for in the *Privacy Act 1988* are not diminished.**

15.44 The committee notes that the absence of a prescribed timeframe in which organisations are required to respond to requests for access. It considers that this appears to be inconsistent with the spirit of the principle as outlined in the Companion Guide, in that individuals are to be provided with the right of access to their personal information. While some submitters called for a fixed timeframe to be applied to organisations, the committee notes the comments by the Office of the Privacy Commissioner in relation to guidance already provided by the office and the suggestion that a note be added to APP 12(4)(a). The committee agrees with the comments of the Office of the Privacy Commissioner and recommends that a note be added to APP 12(4)(a) to clarify that a reasonable period of time in which an organisation must respond to a request for access would not usually be longer than 30 days.

15.45 In relation to access charges, the Law Institute of Victoria recommended that the costs clause in APP 12(8) be amended from organisations not charging 'excessive' fees to charging fees 'reasonably necessary to recoup costs incurred by the entity'.[43] Such an amendment would permit organisations to recoup actual costs but not

43 Law Institute of Victoria, *Submission 36*, p. 8.

unreasonable amounts or profiteer. The committee therefore supports the Law Institute's recommendation.

Recommendation 27

15.46 The committee recommends that a note be added to proposed APP 12(4)(a) to clarify that a reasonable period of time in which an organisation must respond to a request for access would not usually be longer than 30 days.

Recommendation 28

15.47 The committee recommends that APP 12(8) be amended so that it is made clear that access charges imposed by organisations should only be charged at a level reasonably necessary to recoup costs incurred by the entity.

15.48 The committee also notes that the exposure draft on the powers and functions of the Australian Information Commissioner will clarify the enforcement aspects of the access and correction principles in light of moving from the Freedom of Information regime to the privacy regime.

Chapter 16

Australian Privacy Principle 13–correction of personal information

Introduction

16.1 Australian Privacy Principle 13 (APP 13) defines when, and how, individuals can have personal information which is held about them corrected if it is inaccurate, out-of-date, incomplete or irrelevant. The Companion Guide notes that online technological advances are allowing individuals greater ease in gaining access to their own personal information through personal profiles on websites. The Companion Guide commends the online personal profile approach as 'good privacy practice' as it 'ensures individuals have control of their personal information'.[1]

Background

16.2 Access to, and correction of, personal information held by agencies is currently regulated by a combination of provisions of the *Freedom of Information Act 1982* (FOI Act) and Information Privacy Principles 6 and 7 (IPP 6 and IPP 7). IPP 7 provides that an agency must take such steps, if any, as are reasonable to ensure that personal information recorded is accurate and relevant, up-to-date, complete and not misleading. This provision is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendments of documents. IPP 7 also provides that, if the agency is not willing to amend a record as requested by an individual, then the individual may request that a statement be attached to the record and the agency must take reasonable steps to comply with this request.

16.3 Access to, and correction of, personal information held by organisations is currently regulated under National Privacy Principle (NPP 6). NPP 6.5 provides that an organisation must take reasonable steps to correct personal information that it holds, if the individual to whom it relates is able to establish that it is not accurate, complete and up-to-date. If there is a disagreement about the accuracy of the information, the individual may request that the organisation attach a statement to the information and the organisation must take reasonable steps to do so.[2]

16.4 The Australian Law Reform Commission (ALRC) recommended that the access and correction principles be formulated to apply to both agencies and

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, pp 14–15.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 973–74.

organisations in one unified principle.[3] The ALRC also addressed the following issues:

- the criteria by which personal information is assessed as being 'correct', including how these criteria are assessed;
- any burden of proof an individual must meet to establish that personal information that an agency or organisation holds about him or her is not 'correct';
- the manner of correcting personal information that has been found not to meet the correction criteria; and
- the relationship between the correction requirements under the Privacy Act and other federal laws.[4]

16.5 The ALRC accepted that individuals should be provided with the right to correct personal information held about them by agencies and organisations where the information is misleading or not accurate, relevant, up-to-date or complete. The ALRC noted that while these elements are the same as those in the IPPs, they impose two additional elements on organisations – the elements of 'relevant' and 'not misleading'.[5]

16.6 In relation to the burden of proof to establish that personal information is not correct, the ALRC noted that IPP 7 and NPP 6 contain different obligations: the NPP requires that the individual to whom the information relates must establish that it is not accurate, complete and up-to-date, while the IPP places a positive obligation on agencies to take steps to ensure that the personal information they hold is correct. The ALRC concluded that the provisions of the NPP results in uncertainty in the event of a complaint and, therefore, the positive obligation to hold correct personal information should apply to both agencies and organisations. In addition, the ALRC stated that it did not anticipate that this change 'will affect significantly the practical operation of the correction requirements for organisations'.[6]

16.7 There are a number of ways in which personal information may be corrected including by amending the record, deleting the incorrect material or adding to the material. The ALRC recommended that the Office of the Privacy Commissioner (OPC) develop guidance to address the manner in which personal information can be corrected. The ALRC also commented that guidance should discuss potential conflicts

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 974–977.

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 994.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 996.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 999.

between the requirements of the principle and other record keeping obligations including those under the *Archives Act 1983*.[7]

16.8 In addition, the ALRC considered the issue of notification of third parties where an entity has corrected personal information. This matter was discussed widely with stakeholders during the review, with the ALRC concluding that if an entity has corrected information it should be required to notify any other entities to which it has disclosed the information of the correction, if requested to do so by the individual. While stakeholders raised concerns about the cost this requirement may impose on entities, the ALRC was of the view that the 'reasonable steps' requirement would offer sufficient flexibility to cover all situations adequately.[8]

16.9 Other issues addressed by the ALRC were as follows:

- in relation to a statement provided by an individual concerning disputed information, the ALRC was of the view that the statement should be 'associated' with relevant record, as provided for in NPP 6 rather than 'attached' to the relevant record as provided for in IPP 7;[9] and
- where an entity has made a decision to refuse to correct personal information, procedural fairness requires that the individual should be provided with the reasons for an adverse decision as well as the avenues for complaint.[10]

Government response

16.10 The Government accepted that the right of an individual to access and correct personal information should apply to both agencies and organisations and that it be provided for under a single principle. In relation to the correction element of the principle, the Government accepted the recommendation in relation to correction of information and notification of third parties. The Government accepted in principle the ALRC's recommendation relating to the association of a statement with a record which contains personal information which the entity is not willing to correct, if requested to do so by the individual concerned. However, in the Government's view the part of the recommendation referring to agencies was unnecessary because of impending amendments to the FOI Act.[11]

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1000.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1004.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1007.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1016–17.

11 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, pp 69–70.

16.11 The ALRC's recommendation that when an entity refuses to make corrections, the entity must notify the individual of the reasons for the refusal and of potential avenues for complaint was accepted with amendment. The Government noted that the principle should explicitly provide for situations where providing reasons for the refusal to make corrections would undermine the reasons for denying the request, for example, in instances where providing information to the individual would prejudice a criminal investigation.[12]

Issues

16.12 Submitters generally supported the provisions of APP 13.[13] Yahoo!7, for example, noted that APP 13 'recognises that the timing and nature of consent will require a flexible approach'.[14] Similarly, Westpac supported the approach of 'reasonableness' when determining timeframes for responses to individuals, rather than the inclusion of specified timeframes. Westpac further suggested that the OPC work closely with industry in developing flexible and appropriate guidance on applying 'reasonableness' to response timeframes.[15] The Office of the Health Services Commissioner (OHSC), Victoria, also supported the correction principle and noted that APP 13 is consistent with current standards under the *Health Records Act (Vic)*.[16]

16.13 However, the National Australia Bank (NAB) identified two concerns with APP 13: first, the new obligation that where an entity is satisfied that information held is inaccurate, out-of-date, incomplete or irrelevant (APP 13(1)(b)(i)) it must take steps to correct the information. NAB argued that this may conflict with the obligation in APP 3(5) to only collect information from the individual (unless unreasonable or impractical to do so) and gave the example of an entity learning from a third party that information is inaccurate or out-dated. Secondly, NAB submitted that it should not be open to individuals to determine or decide whether an entity holds 'relevant' information as individuals cannot be expected to know or decide on behalf of an entity what types of information are relevant for it to hold (APP 13(1)(b)(ii)).[17] NAB gave the example of a former address which may be irrelevant for some purposes but relevant for others. NAB concluded that 'the protections sought by this reform are already inherent within draft Australian Privacy Principles 3 and 11 in prohibiting entities from collecting "unnecessary" information and in the obligation to destroy or de-identify information if it is no longer needed for any purpose'.[18]

---

12 Australian Government, *Enhancing National Privacy Protection*, p. 71.

13 Australian Institute of Credit Management, *Submission 8*, p. 4; Office of the Health Services Commissioner, *Submission 26*, p. 6.

14 Yahoo!7, *Submission 20*, p. 3.

15 Westpac, *Submission 13*, p. 3.

16 Office of the Health Services Commissioner, *Submission 26*, p. 6.

17 See also The Communications Council, *Submission 23*, p. 8.

18 National Australia Bank, *Submission 2*, pp 5–6.

16.14 Privacy Law Consulting Australia raised issue with 'correcting' information to ensure that it is relevant. Privacy Law Consulting Australia argued that:

> It is unclear what is meant by "correct" in this context since privacy issues posed by use of irrelevant information are not addressed through correction. The terminology should be amended accordingly.[19]

Correction–APP 13(1)

16.15 In relation to APP 13(1) – the obligation to ensure that personal information is accurate, up-to-date, complete and relevant – comments went to the compliance burden and the need to include 'misleading' information in this APP.

16.16 Coles Supermarkets (Coles) voiced concern about the burden imposed by the obligation. Coles noted that it relies on information that it collects being accurate at the time of its collection. It has processes that enable individuals to contact Coles or access Coles' systems to correct errors in their personal information. However, given the size of its operations, Coles commented that it is likely that it would be impractical to check the ongoing accuracy of personal information it has collected.[20]

16.17 The Australian Bankers' Association (ABA) argued that the obligation to correct information may be interpreted in such a way as to require an entity to 'continuously monitor and review personal information that it holds whether prompted to do so or not'. The ABA went on to comment that it did not believe that this was the intention of this principle and sought clarification. The ABA also submitted that banks should be able to comply with this obligation through appropriate review processes, reasonably designed to address the risk of obsolete information being used inappropriately. Otherwise:

> ...the costs to banks of routinely reviewing personal information held by them compared to the negligible benefit to their customers would be unjustifiable on any costs and benefits assessment.[21]

16.18 The Financial Services Council suggested that entities should be obliged to correct personal information only when requested by the individual as 'this ensures that the individual has confirmed that the information is inaccurate and should be amended or deleted'.[22]

16.19 Both the OPC and the Office of the Information Commissioner, Queensland, (OIC) noted that APP 13 does not include a reference to 'misleading' personal information. The OPC noted that ALRC's accepted by the Government proposed that

---

19 Privacy Law Consulting, *Submission 24*, p. 9.

20 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 4.

21 Australian Bankers' Association, *Submission 15*, p. 15.

22 The Financial Services, *Submission 34*, p. 4.

'misleading' information should also be corrected.[23] The OIC commented that situations may arise where information may be correct, up-to-date and complete, but may still create a misleading impression in the mind of a reader. The OIC went on to comment:

> There is a distinction between a misleading impression and an inaccuracy, although there will often be significant overlap; inaccurate facts may well be misleading. However, accurate facts may also give a misleading impression, either because they are incomplete or because the language used in recording the facts could convey a misleading impression.[24]

16.20 The OPC concluded that it may be preferable to include the term 'misleading'.[25]

16.21 In response to concerns that 'misleading' information may not be caught within this obligation, the Department of the Prime Minister and Cabinet (the department) acknowledged that the ALRC recommended a 'misleading' element be included within the 'Access and Correction' principle. However, the department went on to state that:

> During the course of drafting the provisions, it became clear that it was not necessary to include "misleading" as it was covered by "accurate" and "relevant", and it would create an inconsistency with APP 10 about quality of personal information, in which entities have to ensure the personal information they use or disclose is "accurate, up-to-date, complete and relevant".[26]

Notification of correction to third parties–APP 13(3)

16.22 Similar to the comments received about APP 13(1), submitters raised concern about the compliance burden imposed by the obligation to notify third parties of correction to personal information when requested to do so by an individual. In addition, submitters commented on the need for an individual to request notification of third parties and the potential for frivolous or unduly onerous requests.

16.23 Coles argued that the obligation to advise individuals and third parties of corrections under APP 13(3) is 'likely to be administratively burdensome for large organisations with automated systems and raises real concerns regarding compliance and the cost of compliance with these obligations for organisations like Coles'.[27] This concern was supported by the Communications Council which stated that such an

---

23 Office of the Privacy Commissioner, *Submission 39*, p. 42.

24 Office of the Information Commissioner, Queensland, *Submission 18*, p. 6.

25 Office of the Privacy Commissioner, *Submission 39*, p. 42.

26 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 29.

27 Coles Supermarkets Australia, *Submission 10*, p. 4.

obligation 'raises real concerns regarding compliance costs'.[28] The Law Council of Australia (LCA) added its concern on this issue and commented that the obligation to notify third parties would not only impose a 'potentially heavy burden', but also may actually discourage entities from keeping records of disclosures, so as to make it 'impracticable' to notify third party entities of corrections.[29]

16.24 Privacy Law Consulting Australia also suggested that, for many entities, updating policies, procedures and systems to record the parties to whom information is disclosed would be a logistically complex and financially burdensome process. Privacy Law Consulting Australia suggested that:

> ...to ensure entities are not put to unnecessary expense in the belief that a higher level of obligation exists than that which actually applies, the meaning of "reasonable in the circumstances" and "impracticable" should be clarified.[30]

16.25 The Financial Services Council (FSC) raised a concern similar to that raised by Privacy Law Consulting Australia: in order to comply with APP 13(3), entities would need to maintain lists of third party disclosures, and of the particular personal information disclosed. The FSC considered maintaining such lists would 'create a particularly onerous administrative burden on FSC members, and is likely to result in significant compliance costs for the financial services industry'.[31]

16.26 Qantas submitted that an exception should be added to APP 13(3), regulating 'frivolous or unduly onerous requests':

> To prevent the scope for misuse, Qantas submits that there should be exceptions for frivolous or unduly onerous requests. For example, in the case of a name change due to marriage, the responsibility to notify such changes to relevant parties should remain with the individual, rather than the entity.[32]

16.27 The department responded to concerns about compliance burden and commented that it believed that the qualifications in APP 13(3) of 'reasonable steps (if any)' and 'practicability' will provide the necessary flexibility in the obligation to ensure it does not create an onerous compliance burden. In addition, it is anticipated that guidance from the Australian Information Commissioner (AIC) will be necessary to assist agencies and organisations to comply with the obligation.

16.28 The department noted that the ALRC report found factors that should be addressed when assessing whether it would be reasonable and practicable to notify

---

28 The Communications Council, *Submission 23*, p. 8.

29 Law Council of Australia, *Submission 31*, p. 7.

30 Privacy Law Consulting, *Submission 24*, p. 9.

31 Financial Services Council, *Submission 34*, p. 4.

32 Qantas, *Submission 38*, p. 8.

third parties that it has disclosed incorrect information. These factors include whether the agency or organisation has an ongoing relationship with the entity to which it has disclosed the information, the materiality of the correction, the length of time that has elapsed since the information was disclosed and the likelihood that it is still in active use by the third party, the number of entities that would need to be contacted by the agency or organisation and the potential consequence for the individual of the use and disclosure of the incorrect information.[33]

16.29 Professor Graham Greenleaf and Mr Nigel Waters supported the obligation to notify third parties, however, they submitted that 'it still leaves it to the individual to identify the recipient, rather than to request "please notify all previous recipients of the incorrect information".'[34] This matter was also the subject of comment by the Law Institute of Victoria (LIV). The LIV stated:

> The LIV questions why an individual should have to request this notification, particularly where the individual is unaware of the error or to whom the entity has disclosed information or even that information has been disclosed. Entities should be expected to have better records of disclosures to other entities than individuals. The LIV therefore submits that the obligation should be on entities to notify everyone to whom it has disclosed information of the correction.[35]

Refusal to correct information

16.30 Telstra submitted that the obligation on entities under APP 13(4) to provide individuals with written notification of refusals to correct information would render the process of refusing to make corrections more complex than need be and commented that 'in our experience a refusal to correct information is often quite straight forward and a verbal explanation of the reasons would be sufficient'. Telstra suggested that entities should provide individuals with written notice of refusals only when the individual requests written notification. Providing automatic written notification at every instance 'would slow down the process and more than likely inconvenience the person while increasing the compliance burden on us'.[36]

16.31 The LIV suggested that additional guidance be provided on the grounds for entities to refuse to make corrections.[37]

Conclusion

16.32 The Government response to the ALRC recommendations indicated that it accepted that a unified 'Access and Correction' principle shall apply to both agencies

---

33 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 29.

34 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 16.

35 Law Institute of Victoria, *Submission 36*, p. 8.

36 Telstra Corporation Ltd, *Submission 19*, pp 4–5.

37 Law Institute of Victoria, *Submission 36*, p. 8.

and organisations. However, the exposure draft provides for separate access and correction principles. The committee supports this change as it provides clear and easy reference to the obligations to correct personal information if it is inaccurate, out-of-date, incomplete or irrelevant.

16.33 In relation to the inclusion of the term 'misleading' in APP 13, the committee notes that both the OIC and OPC supported this approach. Submitters also pointed out that the term 'misleading' is currently contained in IPP 7 and was included in the ALRC's recommended 'Access and Correction' privacy principle UPP 9. The committee notes that the department's comments that it found that the term 'misleading' was not necessary as 'misleading information' could be covered by 'accurate' and 'relevant' and its inclusion would lead to an inconsistency with APP 10. However, the ALRC considered the effect of differences that would arise between the 'Access and Correction' principle and the 'Data Quality' principle (APP 10) if the term misleading was used in the 'Access and Correction' principle and stated that it 'considers this discrepancy to be appropriate, however, in light of the different context in which these principles operate'.[38] In addition, the credit reporting exposure draft contains reference to 'misleading' information. Therefore, the committee remains to be persuaded by the department's argument in relation to this matter and considers that the decision to omit the term 'misleading' from APP 13 should be re-considered.

Recommendation 29

16.34 That the decision to omit the term 'misleading' in APP 13, relating to the correction of personal information, be reconsidered.

16.35 The committee acknowledges concerns raised in submissions that the obligations contained in APP 13(1) and APP 13(3) may increase compliance burdens for entities, in particular large commercial organisations. However, the committee supports the ALRC's and Government's view that an individual has a right to correct personal information held by an entity and that the correction should be made known to third parties if requested by the individual.[39] While there may be an increased compliance burden in some instances, both APP 13(1) and APP 13(3) contain the qualification of 'reasonable steps (if any)' and 'practicability'. The committee considers that the inclusion of these qualifications will allow sufficient flexibility (including the option not to take any steps) to ensure that compliance does not become overly burdensome. The committee therefore regards the current wording of APP 13(1) and APP 13(3) adequately balances the interests of individuals and the concerns of entities.

38 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 997.

39 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1004.

Chapter 17

Committee conclusions

17.1 The reform of privacy law in Australia is a substantial undertaking. The Australian Law Reform Commission's (ALRC) review took 28 months to complete, addressed a multitude of issues and resulted in the publication of a three-volume report. The Australian Privacy Principles (APP) exposure draft is the first stage of the reform process to be considered.

17.2 The Government accepted the majority of the ALRC's recommendations in relation to the privacy principles. Indeed, Professor Rosalind Croucher, President, ALRC, commented at the committee's hearing that the APPs 'are consistent with and flow from the recommendations that the ALRC made in *For your information'*.[1] Although the ALRC indicated that there were a number of matters where the APPs diverge from the recommendations made in the review report, Professor Croucher stated:

> But the gist of the privacy principles is a very good one. It places the idea of privacy principles as a unified presentation. We congratulate the initiative and encourage the implementation of those privacy principles as a national initiative as a priority.[2]

17.3 While many submitters welcomed the reforms, the committee received a range of views on whether or not the APPs meet the objectives underpinning the need for reform and provide greater privacy protection. In addressing this point, the Office of the Privacy Commissioner (OPC) commented that the reform process should ensure that:

- there is a streamlined, single set of principles for the public and private sectors, which promote national consistency;
- privacy rights and obligations are simplified and therefore easy to understand and apply;
- existing privacy protections are maintained, not diminished; and
- a high-level, principles-based, technology-neutral approach is adopted that is capable of protecting and promoting individuals' privacy into the future.[3]

17.4 The APP exposure draft provides for a single set of principles applying to all entities to replace the Information Privacy Principles which apply to agencies and the

---

1 Professor Rosalind Croucher, President, ALRC, *Committee Hansard*, 25 November 2010, p. 1.

2 Professor Rosalind Croucher, President, ALRC, *Committee Hansard*, 25 November 2010, p. 1.

3 Office of the Privacy Commissioner, *Submission 39*, p. 5.

National Privacy Principles which apply to organisations. As noted by Professor Croucher:

> Where you have two sets of principles, there is an opportunity for confusion about what, for instance, government agencies and also those employers covered by the existing principles have to do, and where there is confusion there is the possibility of an imperfect protection and an imperfect respect for the fundamental protection of personal information. In that context, the development of a unified set of principles would only improve the ability for those governed by it to discharge the responsibility under them.[4]

17.5 The committee acknowledges that drafting a single set of APPs was a particularly complex task. The need to consolidate the IPPs and the NPPs, while at the same time taking into account the ALRC's recommendations accepted by the Government and additional matters announced by the Government, has resulted in very long APPs. In itself, the length of the exposure draft is not of concern: short does not always mean simple or easy to understand. However, the committee is concerned that many submitters stated that the APPs are complex, dense, and difficult to understand. In particular, the committee has noted the view of the Office of the Privacy Commissioner (now the Office of the Australian Information Commissioner) that the APPs should be simplified to improve clarity. The committee considers that this is a significant issue: without clarity, agencies and organisations may find it difficult to comply with their privacy obligations and individuals may not understand how their privacy is protected. As a consequence, the committee has made recommendations to simplify the structure of the APPs, and to improve clarity.

17.6 Evidence received by the committee expressed the opinion that there had been a diminution of privacy protections in some instances. The committee has noted the comments of the Department of the Prime Minister and Cabinet that 'the comments in a lot of the submissions are really around alternative ways of how it might have been done' but the approach taken has not led to any diminution of protections for privacy in Australia. The department also pointed to particular examples of enhanced protections, for example the expansion to Commonwealth agencies of the cross-border disclosure of personal information principle (APP 8).[5]

17.7 While it is the case that there are alternative approaches to the way the principles could be framed, the committee was concerned that there may be some instances where privacy protection may have been inadvertently compromised, for example, APP 3 (collection of solicited information). Therefore, the committee has recommended the re-consideration of some principles to ensure that privacy protections are not diminished. However, on balance, the committee considers that privacy protections have not been weakened and welcomes the enhancement of the privacy regime through the new principles for open and transparent management of

---

4 Professor Rosalind Croucher, President, ALRC, *Committee Hansard*, 25 November 2010, p. 5.

5 Ms Joan Sheedy, Department of the Prime Minister and Cabinet, *Committee Hansard*, 25 November 2010, p. 13.

personal information and cross-border disclosure, more specific regulation of direct marketing activities and restrictions on the use of government issued identifiers.

17.8 A further matter of concern to submitters was the number of exceptions contained in some of the principles. Submitters commented that a large number of exceptions can undermine the privacy regime and limit accountability. The committee considers that in formulating a single set of privacy principles, that it was perhaps unavoidable that a large number of exceptions were required. However, in light of the concerns raised about the complexity of the APPs the committee has recommended that consideration be given to the suggestion that agency specific matters be dealt with in portfolio legislation. The committee also notes that guidance will be provided by the Office of the Australian Information Commissioner in relation to a range of exceptions. The committee considers that guidance will ensure that exceptions are used appropriately.

17.9 The committee considers that it is important that entities have in place internal policies and practices that enable compliance with the privacy principles. The new requirements for privacy policies will enable individuals to access additional information in relation to complaint handling processes and the countries where personal information is transferred to overseas recipients. There was considerable comment from organisations about these requirements and the compliance burden that may arise. The committee acknowledges that in some instances the compliance burden may increase however, the committee is of the view that the benefits of the additional requirements outweigh the compliance costs. In addition, the committee notes that many principles include a 'reasonableness' test for the matters or steps to be undertaken and, in some principles, the test also provides that no steps need be taken if it is reasonable in the circumstances. The committee considers that these provisions provide entities with sufficient flexibility in complying with the privacy regime.

17.10 In conclusion, the committee considers that notwithstanding the recommendations made by the committee, the APPs contained in the exposure draft reflect the intent of the ALRC review and the needs of the Government to ensure that standards are in place to address the risk of harm from the inappropriate collection, use and disclosure of personal information and to meet the expectations of individuals that personal information will be handled appropriately. The APPs also address community concerns arising from the cross-border disclosure of personal information and balance the public's and the individual's interest in efficient and effective service delivery and public safety.

Senator Helen Polley
Chair

APPENDIX 1

Submissions and Additional Information received by the Committee

Submissions

1 Australian Law Reform Commission
2 National Australia Bank
3 Confidential
4 Office of the Guardian for Children and Young People
5 Office of the Victorian Privacy Commissioner
6 NAID-Australasia
7 Abacus Australian Mutuals
8 Australian Institute of Credit Management
9 Epworth Health Care
10 Coles Supermarkets Australia
11 Dr Colin Bennett
12 Australian Finance Conference
13 The Westpac Group
14 Microsoft Australia
15 Australian Bankers' Association
16 Google Australia and New Zealand
17 Insurance Council of Australia
18 Office of the Information Commissioner - Queensland
19 Telstra Corporation
20 Yahoo!7
21 Australian Association of National Advertisers
22 Australian Hotels Association
23 The Communications Council
24 Privacy Law Consulting Australia
25 Professor Graham Greenleaf and Mr Nigel Waters
26 Office of the Health Services Commissioner
27 Australian Direct Marketing Association

28 Deliotte Touche Tohmatsu

29 Privacy NSW

30 Name Withheld

31 Law Council of Australia

31a Supplementary Submission from the Law Council of Australia

32 Public Interest Advocacy Centre

33 Australian Privacy Foundation

34 Financial Services Council

35 Catholic Education Office - Archdiocese of Melbourne

36 Law Institute of Victoria

37 Australian Medical Association

38 Qantas Airways

39 Office of the Privacy Commissioner (now the Office of the Australian Information Commissioner)

40 Obesity Policy Coalition

41 Internet Society of Australia

42 NSW Department of Justice and Attorney General

43 Macquarie Telecom

44 Mr Rodney Lovell

45 Confidential

Additional Information

1 Background information provided by the Department of the Prime Minister and Cabinet

2 Dr Normann Witzleb, Faculty of Law, Monash University 'Privacy: Exposure Draft of the new Australian Privacy Principles – The first stage of reforms to the *Privacy Act 1988* (Cth)', *Australian Business Law Review* 39 (2011)

Answers to Questions on Notice

1 Australian Law Reform Commission: Answers to Questions on Notice provided following the public hearing on 25 November 2010, dated 15 March 2011

2 Department of the Prime Minister and Cabinet: Answers to Questions on Notice (questions 1 to 60) provided following the public hearing on 25 November 2010

APPENDIX 2

Public Hearing and Witnesses

Thursday, 25 November 2010
Committee Room 2S1, Parliament House, Canberra

Committee Members in attendance

Senator Helen Polley (Chair)
Senator Mitch Fifield (Deputy Chair)
Senator the Hon Brett Mason

Witnesses

Australian Law Reform Commission *via teleconference*

Professor Rosalind Croucher, President
Mr Bruce Alston, Senior Legal Officer

Department of the Prime Minister and Cabinet

Ms Philippa Lynch, First Assistant Secretary Government Division
Ms Joan Sheedy, Assistant Secretary, Privacy and FOI Policy Branch
Mr Colin Minihan, Senior Advisor, Privacy and FOI Policy Branch
Ms Janine Ward, Senior Advisor, Privacy and FOI Policy Branch

APPENDIX 3

Information Privacy Principles and National Privacy Principles

Information Privacy Principles (*Privacy Act 1988*, section 14)

Principle 1

Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
   (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4

Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5

Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
   (a) whether the record-keeper has possession or control of any records that contain personal information; and
   (b) if the record-keeper has possession or control of a record that contains such information:
      (i) the nature of that information;
      (ii) the main purposes for which that information is used; and
      (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:
   (a) the nature of the records of personal information kept by or on behalf of the record-keeper;
   (b) the purpose for which each type of record is kept;
   (c) the classes of individuals about whom records are kept;
   (d) the period for which each type of record is kept;
   (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
   (f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:
   (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
   (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6

Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7

Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
   (a) is accurate; and
   (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 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.

3. Where:
   (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
   (b) 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 record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8

Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9

Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10

Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
   (a) the individual concerned has consented to use of the information for that other purpose;
   (b) the record-keeper believes on reasonable grounds that 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;
   (c) use of the information for that other purpose is required or authorised by or under law;
   (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
   (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

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

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

National Privacy Principles (*Privacy Act 1988,* Schedule 3)

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

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

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

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

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 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.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

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

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

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

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or

she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

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

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and

(iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; or

(f) the 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; or

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

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

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

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

(iii) the protection of the public revenue;

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

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

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

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to 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.

2.4 Despite subclause 2.1, an 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:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

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

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

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

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child: without limiting who is a child of an individual for the purposes of this clause, each of the following is the ***child*** of an individual:

(a) an adopted child, stepchild, exnuptial child or foster child of the individual; and

(b) someone who is a child of the individual within the meaning of the *Family Law Act 1975*.

de facto partner has the meaning given by the *Acts Interpretation Act 1901*.

parent: without limiting who is a parent of an individual for the purposes of this clause, someone is the ***parent*** of an individual if the individual is his or her child because of the definition of ***child*** in this subclause.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

stepchild: without limiting who is a stepchild of an individual for the purposes of this clause, someone is the ***stepchild*** of an individual if he or she would be the individual's stepchild except that the individual is not legally married to the individual's de facto partner.

2.7 For the purposes of the definition of ***relative*** in subclause 2.6, relationships to an individual may also be traced to or through another individual who is:

(a) a de facto partner of the first individual; or

(b) the child of the first individual because of the definition of ***child*** in that subclause.

2.8 For the purposes of the definition of ***sibling*** in subclause 2.6, an individual is also a sibling of another individual if a relationship referred to in that definition can be traced through a parent of either or both of them.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 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.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(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; or

(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; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(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; or

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

(iii) the protection of the public revenue; or

(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 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.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 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.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the

information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 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; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an ***identifier***.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(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;

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

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

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required or authorised by or under law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

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

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

APPENDIX 4

Australian Privacy Principles Exposure Draft

EXPOSURE DRAFT

Part A—Australian Privacy Principles

Division 1—Introduction

1 Guide to this Part

Overview

This Part sets out the Australian Privacy Principles.

Division 2 sets out principles that require entities to consider the privacy of personal information, including ensuring that entities manage personal information in an open and transparent way.

Division 3 sets out principles that deal with the collection of personal information including unsolicited personal information.

Division 4 sets out principles about how entities deal with personal information. The Division includes principles about the use and disclosure of personal information.

Division 5 sets out principles about the integrity of personal information. The Division includes principles about the quality and security of personal information.

Division 6 sets out principles that deal with requests for access to, and the correction of, personal information.

Australian Privacy Principles

The Australian Privacy Principles are:

Australian Privacy Principle 1—open and transparent management of personal information

Australian Privacy Principle 2—anonymity and pseudonymity

EXPOSURE DRAFT

Australian Privacy Principle 3—collection of solicited personal information

Australian Privacy Principle 4—receiving unsolicited personal information

Australian Privacy Principle 5—notification of the collection of personal information

Australian Privacy Principle 6—use or disclosure of personal information

Australian Privacy Principle 7—direct marketing

Australian Privacy Principle 8—cross-border disclosure of personal information

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Australian Privacy Principle 10—quality of personal information

Australian Privacy Principle 11—security of personal information

Australian Privacy Principle 12—access to personal information

Australian Privacy Principle 13—correction of personal information

Division 2—Consideration of personal information privacy

2 Australian Privacy Principle 1—open and transparent management of personal information

(1) The object of this principle is to ensure that entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

(2) An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles.

Privacy policy

(3) An entity must have a clearly expressed and up-to-date policy (the ***privacy policy***) about the management of personal information by the entity.

(4) Without limiting subsection (3), the privacy policy must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the privacy policy.

Availability of privacy policy etc.

(5) An entity must take such steps as are reasonable in the circumstances to make its privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

(6) If an individual requests a copy of an entity's privacy policy in a particular form, the entity must take such steps as are reasonable in the circumstances to give the individual a copy in that form.

3 Australian Privacy Principle 2—anonymity and pseudonymity

(1) Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.

(2) Subsection (1) does not apply if:

(a) an entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to deal with individuals who have identified themselves; or

(b) it is impracticable for an entity to deal with individuals who have not identified themselves.

Division 3—Collection of personal information

4 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

(1) An entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

Sensitive information

(2) An entity must not collect sensitive information about an individual unless:
  (a) both of the following apply:
    (i) the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities;
    (ii) the individual consents to the collection of the information; or
  (b) subsection (3) applies in relation to the information.

(3) This subsection applies in relation to sensitive information about an individual (the ***affected individual***) if:
  (a) the collection of the information is required or authorised by or under an Australian law, or an order of a court or tribunal; or
  (b) both of the following apply:
    (i) the entity reasonably believes that the collection of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
    (ii) it is unreasonable or impracticable to obtain the affected individual's consent to the collection; or
  (c) both of the following apply:
    (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the

entity's functions or activities has been, is being or may be engaged in;

(ii) the entity reasonably believes that the collection of the information is necessary in order for the entity to take appropriate action in relation to the matter; or

(d) both of the following apply:

(i) the entity is an enforcement body;

(ii) the entity reasonably believes that the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) both of the following apply:

(i) the entity is an agency;

(ii) the entity reasonably believes that the collection of the information is necessary for the entity's diplomatic or consular functions or activities; or

(f) the entity is the Defence Force and the entity reasonably believes that the collection of the information is necessary for any of the following occurring outside Australia:

(i) war or warlike operations;

(ii) peacekeeping or peace enforcement;

(iii) civil aid, humanitarian assistance, medical or civil emergency or disaster relief; or

(g) both of the following apply:

(i) the entity reasonably believes that the collection of the information is reasonably necessary to assist any entity, body or person to locate a person who has been reported as missing;

(ii) the collection complies with the Australian Privacy Rules made under paragraph 21(a); or

(h) both of the following apply:

(i) the information is collected by a non-profit organisation and relates to the activities of the non-profit organisation;

(ii) the information relates solely to the members of the non-profit organisation, or to individuals who have

regular contact with the organisation in connection with its activities; or

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

(j) the collection of the information is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Means of collection

(4) An entity must collect personal information only by lawful and fair means.

(5) An entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency—the entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to collect the information other than from the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

(6) This principle applies to the collection of personal information that is solicited by an entity.

5 Australian Privacy Principle 4—receiving unsolicited personal information

(1) If:

(a) an entity receives personal information about an individual; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period of receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

(2) The entity may use or disclose the personal information for the purposes of making the determination under subsection (1).

(3) If the entity determines that the entity could have collected the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had so collected the information.

(4) If the entity determines that the entity could not have collected the personal information, the entity must, as soon as practicable but only if it is lawful and reasonable to do so:
  (a) destroy the information; or
  (b) ensure that the information is no longer personal information.

6 Australian Privacy Principle 5—notification of the collection of personal information

(1) At or before the time or, if that is not practicable, as soon as practicable after, an entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:
  (a) to notify the individual of such matters referred to in subsection (2) as is reasonable in the circumstances; or
  (b) to otherwise ensure that the individual is aware of any such matters.

(2) The matters for the purposes of subsection (1) are as follows:
  (a) the identity and contact details of the entity;
  (b) if:
    (i) the entity collects the personal information from someone other than the individual; or
    (ii) the individual may not be aware that the entity has collected the personal information;

  the fact that the entity so collects, or has collected, the information and the circumstances of that collection;
  (c) if the collection of the personal information is required or authorised by or under an Australian law or an order of a court or tribunal—the fact that the collection is so required or authorised (including the name of the Australian law, or

which order of a court or tribunal requires or authorises the collection);

(d) the purposes for which the entity collects the personal information;

(e) the main consequences (if any) for the individual if all or part of the personal information is not collected by the entity;

(f) any other entity, body or person, or the types of any other entities, bodies or persons, to which the entity usually discloses personal information of the kind collected by the entity;

(g) that the entity's privacy policy contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the entity's privacy policy contains information about how the individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;

(i) whether the entity is likely to disclose the personal information to overseas recipients;

(j) if the entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Division 4—Dealing with personal information

7 Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

(1) If an entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subsection (2) applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia.

(2) This subsection applies in relation to the use or disclosure of personal information about an individual (the ***affected individual***) if:

(a) the affected individual would reasonably expect the entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law, or an order of a court or tribunal; or

(c) both of the following apply:

(i) the entity reasonably believes that the use or disclosure of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;

(ii) it is unreasonable or impracticable to obtain the affected individual's consent to the use or disclosure; or

(d) both of the following apply:
  (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
  (ii) the entity reasonably believes that the use or disclosure of the information is necessary for the entity to take appropriate action in relation to the matter; or

(e) the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities by, or on behalf of, an enforcement body; or

(f) both of the following apply:
  (i) the entity is an agency;
  (ii) the entity reasonably believes that the use or disclosure of the information is necessary for the entity's diplomatic or consular functions or activities; or

(g) both of the following apply:
  (i) the entity reasonably believes that the use or disclosure of the information is reasonably necessary to assist any entity, body or person to locate a person who has been reported as missing;
  (ii) the use or disclosure complies with the Australian Privacy Rules made under paragraph 21(b); or

(h) the use or disclosure of the information is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or

(i) the use or disclosure of the information is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Written note of use or disclosure

(3) If an entity uses or discloses personal information in accordance with paragraph (2)(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

(4) If:
  (a) an entity is a body corporate; and
  (b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

(5) This principle does not apply to the use or disclosure by an organisation of:
  (a) personal information for the purpose of direct marketing; or
  (b) government related identifiers.

8 Australian Privacy Principle 7—direct marketing

Direct marketing

(1) If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing unless:
  (a) if the information is sensitive information and paragraph (c) does not apply—the individual has consented to the use or disclosure of the information for that purpose; or
  (b) if the information is not sensitive information and paragraph (c) does not apply—subsection (2) or (3) applies in relation to the use or disclosure of the information for that purpose; or
  (c) if:
    (i) the organisation is a contracted service provider for a Commonwealth contract; and
    (ii) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract;

  the use or disclosure is necessary to meet (directly or indirectly) an obligation under the contract.

Note: An act or practice of an agency may be treated as an act or practice of an organisation.

Personal information collected from the individual

(2) This subsection applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

Personal information collected from another person etc.

(3) This subsection applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) a person other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Individual may request not to receive direct marketing communications etc.

(4) If an organisation uses or discloses personal information about an individual for the purpose of direct marketing by the organisation, or for the purpose of facilitating direct marketing by other organisations, the individual may:

(a) if the organisation uses or discloses the information for the purpose of direct marketing by the organisation—request not to receive direct marketing communications from the organisation; and

(b) if the organisation uses or discloses the information for the purpose of facilitating direct marketing by other organisations—request the organisation not to use or disclose the information for that purpose; and

(c) request the organisation to provide the organisation's source of information.

(5) If an individual makes a request of a kind referred to in subsection (4) to an organisation, the organisation:

(a) must not charge the individual for the making of, or to give effect to, the request; and

(b) if the request is of a kind referred to in paragraph (4)(a) or (b)—must give effect to the request within a reasonable period after the request is made; and

(c) if the request is of a kind referred to in paragraph (4)(c)—must, within a reasonable period after the request is made, notify the individual of the organisation's source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

(6) This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;
(b) the *Spam Act 2003*;
(c) any other Act of the Commonwealth prescribed by the regulations.

9 Australian Privacy Principle 8—cross-border disclosure of personal information

(1) Before an entity discloses personal information about an individual to a person (the ***overseas recipient***):
(a) who is not in Australia; and
(b) who is not the entity or the individual;
the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

(2) Subsection (1) does not apply to the disclosure of personal information about an individual (the ***affected individual***) by an entity to the overseas recipient if:
(a) the entity reasonably believes that:
(i) the overseas recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
(ii) there are mechanisms that the affected individual can access to take action to enforce that protection of the law or binding scheme; or
(b) both of the following apply:
(i) the entity expressly informs the affected individual that if he or she consents to the disclosure of the information, subsection (1) will not apply to the disclosure;
(ii) after being so informed, the affected individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law, or an order of a court or tribunal; or

(d) each of the following applies:
  (i) the entity is an agency;
  (ii) the disclosure of the information is required or authorised by or under an international agreement relating to information sharing;
  (iii) Australia is a party to the international agreement; or

(e) both of the following apply:
  (i) the entity reasonably believes that the disclosure of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
  (ii) it is unreasonable or impracticable to obtain the affected individual's consent to the disclosure; or

(f) both of the following apply:
  (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
  (ii) the entity reasonably believes that the disclosure of the information is necessary for the entity to take appropriate action in relation to the matter; or

(g) each of the following applies:
  (i) the entity is an agency;
  (ii) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities by, or on behalf of, an enforcement body;
  (iii) the overseas recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body; or

(h) both of the following apply:
  (i) the entity is an agency;

(ii) the entity reasonably believes that the disclosure of the information is necessary for the entity's diplomatic or consular functions or activities; or

(i) the entity is the Defence Force and the entity reasonably believes that the disclosure of the information is necessary for any of the following occurring outside Australia:

(i) war or warlike operations;

(ii) peacekeeping or peace enforcement;

(iii) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

10 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

(1) An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law, or an order of a court or tribunal; or

(b) subsection (3) applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation.

Use or disclosure of government related identifiers

(2) An organisation must not use or disclose a government related identifier of an individual (the ***affected individual***) unless:

(a) the use or disclosure of the government related identifier is reasonably necessary for the organisation to verify the identity of the affected individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the government related identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the government related identifier is required or authorised by or under an Australian law, or an order of a court or tribunal; or

(d) both of the following apply:
  (i) the organisation reasonably believes that the use or disclosure of the government related identifier is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
  (ii) it is unreasonable or impracticable to obtain the affected individual's consent to the use or disclosure; or

(e) both of the following apply:
  (i) the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in;
  (ii) the organisation reasonably believes that the use or disclosure of the government related identifier is necessary for the organisation to take appropriate action in relation to the matter; or

(f) the organisation reasonably believes that the use or disclosure of the government related identifier is reasonably necessary for one or more enforcement related activities by, or on behalf of, an enforcement body; or

(g) subsection (3) applies in relation to the use or disclosure.

Note: An act or practice of an agency may be treated as an act or practice of an organisation.

Regulations about adoption, use or disclosure

(3) This subsection applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if each of the following applies:
  (a) the government related identifier is prescribed by the regulations;
  (b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations;
  (c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subsection are prescribed, see subsections 22(2) and (3).

Government related identifier

(4) A ***government related identifier*** of an individual is an identifier of the individual that has been assigned by:

(a) an agency; or

(b) a State or Territory authority; or

(c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or

(d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

Identifier

(5) An ***identifier*** of an individual is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

(6) Despite subsection (5), none of the following is an ***identifier*** of an individual:

(a) the individual's name;

(b) the individual's ABN (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*);

(c) anything else prescribed by the regulations.

Division 5—Integrity of personal information

11 Australian Privacy Principle 10—quality of personal information

(1) An entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the entity collects is accurate, up-to-date and complete.

(2) An entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the entity uses or discloses is accurate, up-to-date, complete and relevant.

12 Australian Privacy Principle 11—security of personal information

(1) If an entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

(2) If:

(a) an entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Division; and

(c) the entity is not required by or under an Australian law, or an order of a court or tribunal, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is no longer personal information.

Division 6—Access to, and correction of, personal information

13 Australian Privacy Principle 12—access to personal information

Access

(1) If an entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

(2) If:
  (a) the entity is an agency; and
  (b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:
    (i) the *Freedom of Information Act 1982*; or
    (ii) any other Act of the Commonwealth that provides for access by persons to documents;

then, despite subsection (1), the entity is not required to give access to the extent that the entity is so required or authorised.

Exception to access—organisation

(3) If the entity is an organisation then, despite subsection (1), the entity is not required to give the individual access to the personal information to the extent that:
  (a) the entity reasonably believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; or
  (b) giving access would have an unreasonable impact on the privacy of other individuals; or
  (c) the request for access is frivolous or vexatious; or
  (d) the information:
    (i) relates to existing or anticipated legal proceedings between the entity and the individual; and

(ii) would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law, or an order of a court or tribunal; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities by or on behalf of an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

(4) If an individual requests an entity to give access to personal information about the individual, the entity must:

(a) respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

(5) If:

(a) an individual requests an entity to give access to personal information about the individual; and

(b) the entity refuses:

(i) to give the individual access to the information because of subsection (2) or (3); or

(ii) to give access to the information in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access to the information in a way that meets the needs of the entity and the individual.

(6) Without limiting subsection (5), access may be given through the use of a mutually agreed intermediary.

Access charges

(7) If:

(a) an entity is an agency; and

(b) an individual requests the entity to give access to personal information about the individual;

the entity must not charge the individual for the making of the request or for giving access to the information.

(8) If:

(a) an entity is an organisation; and

(b) an individual requests the entity to give access to personal information about the individual; and

(c) the entity charges the individual for giving access to the information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to provide access

(9) If:

(a) an individual requests the entity to give access to personal information about the individual; and

(b) the entity refuses:

(i) to give the individual access to the information because of subsection (2) or (3); or

(ii) to give access to the information in the manner requested by the individual;

the entity must, in writing:

(c) give reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(d) notify the individual of the mechanisms available to complain about the refusal; and

(e) inform the individual of any other matter prescribed by the regulations.

14 Australian Privacy Principle 13—correction of personal information

Correction

(1) If:

(a) an entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete or irrelevant; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete and relevant.

Dealing with requests for correction

(2) If an individual requests an entity to correct personal information about the individual, the entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request or for correcting the information.

Notification of correction to third parties

(3) If:

(a) an entity corrects personal information about an individual that the entity previously disclosed to another entity; and

(b) the individual requests the entity to notify the other entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

(4) If:

(a) an individual requests an entity to correct personal information about the individual; and

(b) the entity refuses to correct the information;

the entity must, in writing:

(c) give reasons for the refusal except to the extent that it would be unreasonable to do so; and

(d) notify the individual of the mechanisms available to complain about the refusal; and

(e) inform the individual of any other matter prescribed by the regulations.

Request to associate a statement

(5) If:

(a) an individual requests an entity to correct personal information about the individual; and

(b) the entity refuses to correct the information; and

(c) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete or irrelevant;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

(6) If an individual requests an entity to associate a statement with personal information about the individual, the entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request or for associating the statement with the information.