The Senate

Environment and Communications References Committee

The adequacy of protections for the privacy of Australians online

April 2011

ISBN 978-1-74229-427-8

This document was printed by the Senate Printing Unit, Parliament House, Canberra

Committee membership

Committee members to 27 September 2010
Senator Mary Jo Fisher (LP, SA) (Chair)
Senator Anne McEwen (ALP, SA) (Deputy Chair)
Senator the Hon. Ron Boswell (NATS, QLD)
Senator Scott Ludlam (AG, WA)
Senator the Hon. Judith Troeth (LP, VIC)
Senator Dana Wortley (ALP, SA)

Committee members from 30 September 2010
Senator Mary Jo Fisher (LP, SA) (Chair)
Senator Doug Cameron (ALP, NSW) (Deputy Chair)
Senator the Hon. Ron Boswell (NATS, QLD)
Senator Scott Ludlam (AG, WA)
Senator the Hon. Judith Troeth (LP, VIC)
Senator Dana Wortley (ALP, SA)

Committee secretariat
Mr Stephen Palethorpe, Secretary
Mr Geoff Dawson, Principal Research Officer
Ms Nina Boughey, Senior Research Officer
Ms Jacquie Hawkins, Research Officer
Mrs Dianne Warhurst, Administrative Officer

Committee address
PO Box 6100
Parliament House
Canberra ACT 2600
Tel: 02 6277 3526
Fax: 02 6277 5818
Email: ec.sen@aph.gov.au
Internet: www.aph.gov.au/senate/committee/ec_ctte/index.htm

Table of Contents

Recommendations

Recommendation 1

2.31 The committee recommends that the government consider and respond to the recommendations in the Cyberspace Law and Policy Centre's report: *Communications privacy complaints: In search of the right path*, and recommendations from the Australian Communications Consumer Action Network arising from that report.

Recommendation 2

3.30 The committee recommends that the Australian Privacy Commissioner's complaint-handling role under paragraph 21(1)(ab) of the Privacy Act be expanded to more effectively address complaints about the misuse of privacy consent forms in the online context.

3.31 The committee further recommends that the Office of the Privacy Commissioner examine the issue of consent in the online context and develop guidelines on the appropriate use of privacy consent forms for online services.

Recommendation 3

3.50 The committee recommends that the small business exemptions should be amended to ensure that small businesses which hold substantial quantities of personal information, or which transfer personal information offshore are subject to the requirements of the *Privacy Act 1988*.

3.51 To achieve this end, the committee urges the Australian Privacy Commissioner to undertake a review of those categories of small business with significant personal data holdings, and to make recommendations to government about expanding the categories of small business operators prescribed in regulations as subject to the *Privacy Act 1988*.

3.52 The committee further recommends that the second tranche of reforms to the *Privacy Act 1988* amend the Act to provide that all Australian organisations which transfer personal information overseas, including small businesses, must ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.

Recommendation 4

3.86 The Committee recommends that the OPC in consultation with web browser developers, ISPs and the advertising industry, should, in accordance with proposed amendments to the Privacy Act, develop and impose a code which includes a 'Do Not Track' model following consultation with stakeholders.

Recommendation 5

3.96 The committee recommends that item 19(3)(g)(ii) of the exposure draft of amendments to the *Privacy Act 1988* be amended to provide that an organisation has an Australian link if it collects information *from* Australia, thereby ensuring that information collected from Australia in the online context is protected by the *Privacy Act 1988*.

Recommendation 6

3.109 The committee recommends that the government amend the *Privacy Act 1988* to require all Australian organisations that transfer personal information offshore are fully accountable for protecting the privacy of that information.

3.110 The committee further recommends that the government consider the enforceability of these provisions and, if necessary, strengthen the powers of the Australian Privacy Commissioner to enforce offshore data transfer provisions.

Recommendation 7

3.116 The committee recommends that the Australian government continue to work internationally, and particularly within our region, to develop strong privacy protections for Australians in the online context.

Recommendation 8

3.122 The committee recommends that the government accept the ALRC's recommendation to legislate a cause of action for serious invasion of privacy.

Recommendation 9

4.74 The committee recommends that before pursuing any mandatory data retention proposal, the government must:

- **undertake an extensive analysis of the costs, benefits and risks of such a scheme;**
- **justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;**
- **quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;**
- **assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and**
- **consult with a range of stakeholders.**

Glossary and acronyms

ACMA	Australian Communications and Media Authority
APPs	proposed Australian Privacy Principles, as set out in the exposure draft of amendments to the *Privacy Act 1988*, released 24 June 2010
cloud computing	the outsourcing of data processing and storage to organisations based overseas
data retention	a proposal from the Attorney-General's Department that would require telecommunications providers, including ISPs, to log and retain certain information on subscribers for local enforcements agencies to access when required
IPPs	Information Privacy Principles, for public sector agencies, established under the *Privacy Act 1988*
ISPs	Internet service providers
NPPs	National Privacy Principles, for private sector organisations, established under the *Privacy Act 1988*
OAIC	Office of the Australian Information Commissioner
OPC	Office of the Privacy Commissioner, integrated into the Office of the Australian Information Commissioner in November 2010
Safe Harbour Principles	process to protect personal information transferred offshore
TIO	Telecommunications Industry Ombudsman

Chapter 1

Introduction

1.1 On 24 June 2010, the Senate referred the matter of the adequacy of protections for the privacy of Australians online to the Senate Environment and Communications References Committee for inquiry and report by 20 October 2010. The reporting date was subsequently extended by the Senate until 22 March, 24 March, and 7 April 2011.

1.2 The terms of reference required that the committee have regard to:

(a) privacy protections and data collection on social networking sites;

(b) data collection activities of private companies;

(c) data collection activities of government agencies; and

(d) other related issues.

Reasons for this inquiry

1.3 The Senate's referral of this inquiry, on the motion of Senator Ludlam, was timely given the significant advances in online technology and computing power over the past decade, many of which have important implications for personal privacy.

1.4 For example, the rapid uptake of social networking technologies since 2002 has substantially expanded the amount and type of personal information that people are sharing online,[1] while improvements in cloud computing technology have made it possible to shift vast quantities of personal data around the world to take advantage of cheap data storage.[2] Technology has also made it possible for companies to monitor the way in which individuals behave online for marketing purposes. A combination of these developments, and other online technological advancements has exacerbated existing concerns with privacy protection in Australia, and in some instances created new concerns.

1.5 Conversely, online technology has also enhanced the ability of individuals and organisations to hide their personal information, including their identity, in certain circumstances. For example, it was reported in *The Age* that 'an industry has now sprung up to protect the identity of those who own dubious websites'.[3] Furthermore, newer communications technologies, such as email, often allow users to remain anonymous, or do not record the same data about individual communications that was

---

1 Friendster was launched in 2002: www.friendster.com/info/index.php (accessed 13 December 2010); Myspace in 2003: Asher Moses, 'MySpace founder takes on Rupert', *Sydney Morning Herald Online*, www.smh.com.au/news/biztech/myspace-founder-takes-on-rupert/2006/11/08/1162661728774.html (accessed 13 December 2010); and Facebook in February 2004: www.facebook.com/press/info.php?factsheet (accessed 13 December 2010).

2 Office of the Privacy Commissioner (OPC), *Submission 16*, pp 21–34.

3 Ian McIlwraith, 'Netting web scammers', *The Age*, 16 September 2010, p. 8.

recorded with conventional technologies, such as telephones. This has created new challenges for law enforcement agencies, as the committee heard in evidence from the Australian Federal Police and Attorney-General's Department.[4]

1.6 The timeliness of the committee's examination of this matter is reflected by the fact that it coincides with a number of reviews of privacy regulation both in Australia and overseas. In June 2010, the Australian Government released an exposure draft of major amendments to the *Privacy Act 1988*, which reflect the first stage of its response to the Australian Law Reform Commission's (ALRC) report on Australian privacy law and practice.[5] The exposure draft was referred to the Senate Finance and Public Administration Legislation Committee for inquiry and report by 1 July 2011.[6]

1.7 The committee understands that the government is also reviewing cyber security and cyber crime in response to the recent House of Representatives committee report *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*.[7] The review will look at the practicality of implementing the recommendations of the Standing Committee's report and will focus on avenues to protect individuals, the community and the private security in the online world. Although the government's review is broader in scope than the committee's inquiry, there may be some common ground, as a secure online environment with adequate privacy will help protect people from identity theft or other online crime involving misuse of personal information.

1.8 The committee's inquiry also coincides with the European Commission's review of the general European Union legal framework on the protection of personal

---

4 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, pp 85–86.

5 Department of the Prime Minister and Cabinet, *Privacy Reforms*, www.alrc.gov.au/publications/report-108 (accessed 9 December 2010); Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, available at www.alrc.gov.au/publications/report-108 (accessed 9 December 2010); and Senator the Hon Joe Ludwig, Cabinet Secretary, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108*, October 2009, available at www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf (accessed 9 December 2010)

6 For information about the Senate Finance and Public Administration Legislation Committee's inquiry see: www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/info.htm (accessed 10 December 2010).

7 House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, June 2010, www.aph.gov.au/house/committee/coms/cybercrime/report.htm (accessed 7 March 2011); and the government response, 25 November 2010, www.aph.gov.au/house/committee/coms/governmentresponses/cybercrime.pdf (accessed 7 March 2011).

data,[8] as well as consideration by the Attorney-General's Department of a mandatory data retention scheme based on that adopted by the EU in 2006.[9]

1.9 Furthermore, in the United States, the Federal Trade Commission released a preliminary report in December 2010 on 'Protecting Consumer Privacy in an Era of Rapid Change' and recommended a framework for businesses and policymakers in dealing with consumer privacy issues.[10]

Conduct of the inquiry

1.10 In accordance with its usual practice, the committee advertised details of the inquiry in *The Australian* on 30 June 2010. The committee also contacted a range of organisations, inviting them to make submissions. The committee received 27 submissions, listed at Appendix 1.

1.11 The committee held two public hearings: in Canberra on 29 October 2010 and in Melbourne on 1 December 2010 (see Appendix 2).

1.12 The committee notes that despite several requests, Facebook failed to provide the committee with any information about its privacy policies and settings in the Australian online environment.

Report structure

1.13 This inquiry raised a diverse range of complex issues related to online technology and privacy. The issues raised were so varied and numerous that it would be impossible to adequately cover them all within the confines of a Senate Committee report. Instead, the committee has identified key themes and recurring issues and synthesised them into a discussion of the major issues confronting privacy regulators with the development of online technologies.

1.14 Broadly, the issues raised fall into two categories: those related to the adequacy of the existing privacy framework for protecting the privacy of Australians online; and challenges for law enforcement arising from technological advances.

---

8 European Commission, *Review of the data protection legal framework*, http://ec.europa.eu/justice/policies/privacy/review/index_en.htm (accessed 10 December 2010). The review has thus far consisted on a stakeholders' conference in May 2009 and further consultations during 2010, and a strategic communication released on 4 November 2010.

9 Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 March 2006 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (accessed 10 December 2010).

10 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010 at www.ftc.gov/os/2010/12/101201privacyreport.pdf (accessed 6 January 2010).

1.15 Chapter 2 of this report outlines the existing privacy framework in Australia, including proposed legislative amendments.

1.16 Chapter 3 discusses the first category of online privacy issues raised during this inquiry—which relate to the adequacy of current and proposed protections for Australians in the online environment. These issues include: the role of consent in Australian privacy law; the small business exemption in the *Privacy Act 1988*; behavioural advertising; the transnational nature of the internet; and whether Australia should enact a statutory cause of action for invasion of privacy.

1.17 Chapter 4 of this report considers the law enforcement challenges arising from technological advances, and specifically the Attorney-General's Department's proposed mandatory data retention scheme.

1.18 Recommendations are addressed either to the Office of the Privacy Commissioner (OPC) or to the government. The committee notes that within government, several different departments will be involved in responding, including the Department of the Prime Minister and Cabinet; the Attorney-General's Department; and the Department of Broadband, Communications and the Digital Economy.

1.19 The OPC was integrated into the Office of the Australian Information Commissioner (OAIC) on 1 November 2010. The Office's submission to this inquiry and the Privacy Commissioner's appearance before this committee both occurred before 1 November 2010, at a time when the Office of the Privacy Commissioner was a stand-alone office. For consistency the report will refer to the Office of the Privacy Commissioner.

Acknowledgments

1.20 The committee would like to thank all of the organisations, individuals and government departments and agencies that contributed to this inquiry. In particular the committee expresses its appreciation to the Attorney-General's Department and the Australian Federal Police for willingly providing the committee with confidential information regarding the proposed data retention proposal.

Chapter 2

Australia's privacy framework

2.1 The Office of the Privacy Commissioner (OPC) submitted that 'the best approach to enhancing privacy online will be multi-faceted'[1] and outlined the components comprising the existing approach to protecting privacy in Australia, which include:

- the *Privacy Act 1988*;
- complaints mechanisms;
- industry self-regulation;
- education;
- privacy enhancing technology; and
- international cooperation.

2.2 Each of these mechanisms is discussed below with a focus on its protection of the privacy of Australians in the online context. Proposed changes to each mechanism are also discussed where relevant.

Legislation

2.3 The key piece of legislation relating to privacy in Australia is the *Privacy Act 1988*. The Privacy Act 'regulates the handling of personal information by most Australian and ACT government agencies, large private sector organisations and some small businesses'.[2]

2.4 The Privacy Act currently contains separate sets of 'privacy principles' for public sector agencies and private sector organisations—the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) respectively.[3] In essence, the principles set out standards for managing and using personal information including collection, use, disclosure, storage and destruction.

2.5 The Privacy Act also established the OPC, recently integrated into the Office of the Australian Information Commissioner (OAIC).[4]

2.6 The OPC submitted that:

> The Privacy Act provides a mechanism to support good personal information handling by government agencies and private sector

---

1 OPC, *Submission 16*, p. 10.

2 OPC, *Submission 16*, p. 10.

3 The NPPs, IPPs and proposed Australian Privacy Principles (APPs) are set out in Appendix 3.

4 *Privacy Act 1988*, Part IV.

> organisations and offers an avenue of redress for individuals that believe that their personal information has been misused.[5]

2.7 The OPC argued that one of the strengths of the Privacy Act is the fact that it uses 'principles' rather than 'prescriptive rules' which has provided a framework that is 'adequately flexible to respond to technological change'.[6] The OPC's submission gives the example of NPP 4.1 which requires private sector organisations to 'take reasonable steps to protect the personal information it holds…'.[7] What constitutes 'reasonable steps' will depend on the circumstances, including the development and availability of new technologies.

2.8 However, despite this inbuilt flexibility, the Australian Law Reform Commission's (ALRC) 2008 review of privacy law and practice in Australia resulted in a range of recommendations as to how the Privacy Act might be improved.[8] The OPC submitted:

> Since its enactment over 20 years ago, the Privacy Act has operated against a backdrop of significant change associated with the information age and the rise of the internet. To ensure the ongoing effectiveness of the Privacy Act in a rapidly evolving technological environment, considerable work has been done in recent years to review and reform the act. Most significantly, the Australian Law Reform Commission undertook a review of privacy—the largest review to date—and the government has provided a first stage response to that review.[9]

2.9 The ALRC's review also examined the role of telecommunications laws in protecting privacy in Australia, and 34 of the recommendations in its 2008 report dealt with the *Telecommunications Act 1997*, *Spam Act 2003* and *Do Not Call Register Act 2006*.[10] The government is yet to respond to these telecommunications-specific recommendations.[11]

2.10 The government has announced that it intends to respond to the ALRC's recommendations in two stages,[12] and has released the first stage of its response.[13]

---

5 OPC, *Submission 16*, p. 8.

6 OPC, *Submission 16*, p. 10.

7 OPC, *Submission 16*, p. 10.

8 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, www.alrc.gov.au/publications/report-108 (accessed 18 January 2011).

9 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 17.

10 Mr Duncan McIntyre, Assistant Secretary, Consumer Policy and Post, Department of Broadband, Communications and the Digital Economy (DBCDE), *Committee Hansard*, 29 October 2010, pp 83–84.

11 Mr Duncan McIntyre, Assistant Secretary, Consumer Policy and Post, DBCDE, *Committee Hansard*, 29 October 2010, pp 83–84.

12 Department of the Prime Minister and Cabinet, 'Privacy Reforms', www.dpmc.gov.au/privacy/reforms.cfm (accessed 14 December 2010).

The government has also released an exposure draft of amendments to the Privacy Act, which is being considered by the Senate Finance and Public Administration Legislation Committee.[14] The key purpose of the exposure draft is to replace the NPPs and IPPs with uniform principles which apply to both the public and private sector—to be called the Australian Privacy Principles (APPs). This reform follows a recommendation by the ALRC and is intended to 'reduce confusion, overlap and inconsistency'.[15]

2.11 The OPC's submission argues that the government's proposed amendments to the privacy principles 'will enhance the operation of the Privacy Act, ensuring it remains effective in the face of continuing technological change'.[16]

2.12 Google agreed that the government's proposed amendments will strengthen the Act:

> We think that the draft privacy legislation currently before the finance and public administration committee is based on a strong principles based framework that has the flexibility to respond to further developments in technology. Another key element of the privacy framework is to have an independent and effective privacy regulator, which is what we believe we have.[17]

2.13 However, other organisations are concerned that the introduction of uniform principles for the public and private sector may weaken privacy protection in Australia. For example, Ms King-Siem, Vice-President, Liberty Victoria noted:

> Having the IPPs and the NPPs originally was a convenient way for the government to introduce regulation of the private sector and take a far softer approach between the private sector and the public sector...there is concern that the APPs are taking a slightly more watered down approach than they could otherwise.[18]

2.14 While many of the proposed amendments to privacy and telecommunications legislation in Australia are relevant to this inquiry, the committee has chosen not to examine the exposure draft in detail given that it is already the subject of another

---

13 Senator the Hon Joe Ludwig, Cabinet Secretary, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108*, October 2009.

14 Senate Finance and Public Administration Legislation Committee, Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm, (accessed 22 October 2010).

15 OPC, *Submission 16*, p. 11.

16 OPC, *Submission 16*, p. 9.

17 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 2.

18 Ms Georgia King-Siem, Vice-President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 20.

Senate committee inquiry. Certain aspects of the proposed legislation, relevant to online privacy specifically, are considered throughout this report, but the committee has not conducted an extensive review of the legislation or proposed amendments as a whole.

2.15 Most States and Territories have legislative privacy protections, with the exceptions of South Australia and Western Australia.[19] Victoria and the ACT also have a right to privacy included in their *Charter of Human Rights and Responsibilities Act 2006* (Vic) and *Human Rights Act 2004* (ACT) respectively.

2.16 However, the OPC noted that:

> Legislation alone is not sufficient to ensure the protection of privacy for Australians online. One reason for this is that domestic laws will not always have jurisdiction in the transnational space of the internet.[20]

Complaints mechanisms

2.17 The Australian Communications Consumer Action Network (ACCAN) submitted that 'complaints are a vital element in privacy protection—indeed, the entire system of privacy protection in the communications sector is built on the receipt and management of complaints'.[21]

2.18 ACCAN recently commissioned the Cyberspace Law and Policy Centre to conduct a research project into privacy complaints in the Australian communications sector which compared complaints made to the OPC, the Australian Communications and Media Authority (ACMA) and the Telecommunications Industry Ombudsman (TIO). Each organisation is responsible for privacy complaints made under different circumstances: the OPC deals with general privacy complaints, and telemarketing and internet related complaints; ACMA deals with spam and do-not-call complaints, plus a small number of general privacy complaints; and the TIO deals with general privacy complaints and internet related complaints.[22]

2.19 The study found vast differences in the number of complaints made to each organisation. In 2009 the ACMA received a total of 16 014 privacy complaints, the TIO received 4942, and the OPC 113.[23] ACCAN acknowledges that the ACMA's jurisdiction over do-not-call register and spam complaints means that it will always receive the highest number of complaints. However, ACCAN noted that the number

---

19 Victorian Privacy Commissioner, *Submission 13*, p. 2.

20 OPC, *Submission 16*, p. 9.

21 ACCAN, *Submission 11*, p. 3.

22 ACCAN, *Submission 11*, pp 3–4; Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 6, at www.cyberlawcentre.org/privacy/ACCAN_Complaints_Report/report.pdf (accessed 23 December 2010).

23 Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 8.

of complaints to the OPC—the major national privacy regulator—is concerningly low.[24]

2.20 The study also found that the average time for dispute resolution was 5 days for the ACMA, 10 days for the TIO and 180 days for the OPC.[25] While noting that 'a small delay is to be expected at the OPC as they have a strong focus on conciliation and some of their matters may be more complex', ACCAN submitted that 'no consumer should be waiting 6 months to have a privacy complaint in the communications sector resolved'.[26]

2.21 In this respect, Ms Teresa Corbin, CEO, ACCAN, emphasised:

> I think it is also important to acknowledge that all these agencies have very different ways of approaching these complaints. For example, one of the reasons the Privacy Commissioner takes longer to deal with these complaints is that they conduct an investigation and conciliation. That is a very different process to an investigation and then making a decision awarding an outcome, which is what the ACMA and the TIO both do, because their powers allow it.[27]

2.22 While the report was generally very positive about the ACMA's complaints handling, the ACMA similarly argued that it is important that the distinct roles of each privacy complaints-handling agency is considered when examining the disparity in resolution timeframes:

> I would just like to draw the distinction that each of us [the ACMA, the OPC and the TIO], when we are working in regulatory spheres, have different responsibilities and different issues that we look at. Some investigations are quite straightforward. Things like the Do Not Call Register are quite straightforward: either somebody is on the register or not on the register or has given consent or not. The Privacy Commissioner, I would expect, would have quite complex investigations from time to time and they always take a bit longer. So, while we welcomed ACCAN's research, as we always do, we felt that there were some areas in there that could have been fleshed out a bit more to point out the differences in people's regulatory responsibilities.[28]

2.23 However, the study also found a range of other issues with the existing privacy complaints structure. For example, the study found that the three complaints pathways also result in disparate outcomes for consumers. ACCAN submitted that while the OPC is able to deliver a complainant compensation or an apology, it will not

---

24 ACCAN, *Submission 11*, pp 4–5.

25 Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 10.

26 ACCAN, *Submission 11*, p. 5.

27 Ms Teresa Corbin, CEO, Australian Communications Consumer Action Network (ACCAN) *Committee Hansard*, 29 October 2010, pp 44–45.

28 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 58.

provide a prompt solution such as immediate correction or removal of personal data. The ACMA is able to deliver prompt corrections, and can also undertake enforcement action, such as fines, but cannot order compensation to a complainant. The TIO can also deliver prompt action and limited enforcement actions.[29] ACCAN argued that this situation is unacceptable and submitted that:

> *Any* privacy complaint in the communications sector lodged with *any* complaints body should be able to achieve all of the outcomes that are desirable in a best practice regulatory environment.[30]

2.24 ACCAN submitted that the information given to consumers about likely resolution times is 'fairly ad hoc and inconsistent', and recommended that this information be made clear to consumers so that they can choose the best avenue to resolve their complaint.[31]

2.25 ACCAN also raised concerns about the accessibility of complaints mechanisms to disadvantaged and vulnerable consumers, but noted that the study was unable to draw conclusions about this issue as no data was kept on the profile of complainants.[32] The CEO of ACCAN, Ms Corbin, stated:

> Obviously, those who are most disadvantaged and vulnerable in our community are also going to be most disadvantaged and vulnerable when it comes to privacy, because a lot of the privacy protection—not waiving rights—revolves around people having high levels of literacy. Clearly, in some of those vulnerable and disadvantaged groups they may well still be using plenty of online services but not necessarily reading everything that goes across the screen. It could well be that they are just using lots of other cues—for example, icons, pictures and video. So, yes, it is a concern and something that we need to do some more work on.[33]

2.26 The Cyberspace Law and Policy Centre made a number of recommendations in its report based on these findings, including: more coordination between the three agencies; consistent messages to consumers and industry; and providing each agency with a full range of regulatory tools.[34]

2.27 Ms Corban informed the committee that ACCAN has approached the OPC with the aim of addressing the issues raised in the study:

> We are hoping it is an opportunity to improve the situation. That is how we have approached the Privacy Commission, although they obviously were not too pleased about our report. We have suggested that, in our dialogue from now on, we actually focus on: why is this the case, how can it be

29 ACCAN, *Submission 11*, p. 6.

30 ACCAN, *Submission 11*, p. 7, emphasis in original.

31 ACCAN, *Submission 11*, p. 6.

32 ACCAN, *Submission 11*, p. 6.

33 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 49.

34 Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 25.

> improved? Also, perhaps it cannot be taken to be exactly the same as the TIO or the ACMA, but how can we actually reduce that time? Or do we need to get more resources to that body? Maybe the new resources that are available because of the information commission will assist there.[35]

2.28 ACCAN has also suggested that the OPC provide more information to consumers about their options, for example by publishing their decisions so that:

> ...then there would be a better awareness of why it takes longer to get an apology than to trigger that enforcement notice. I think there is room for some further explanation from the Privacy Commissioner, but I think there is also some room for improvement, even within the existing powers and structure that they have.[36]

2.29 In response to the Cyberspace Law and Policy Centre's report, the OPC commented:

> The report does not distinguish between the types of privacy complaints received by the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Media and Communications Authority. The Privacy Commissioner can only deal with matters that can be treated as complaints under the *Privacy Act 1988* (Cth). A number of these telecommunications privacy complaints are about credit reporting, which by their nature are complex and generally require detailed investigation.
>
> Nor is it appropriate, without qualification, to compare the investigation times required for complex complaints under the *Privacy Act 1988* with those complaints received under the Spam Act or the Do Not Call Register Act... The Office focuses on working cooperatively with complainants and respondents to resolve complaints through conciliation by achieving outcomes such as apologies, improved business processes, and compensation if appropriate. This negotiation process necessarily takes time.[37]

Committee comment

2.30 The committee urges the government to consider the report of the Cyberspace Law and Policy Centre, and respond to the recommendations made therein, and by ACCAN in response to the report. Specifically, the committee recommends that the government focus on ways to address the inconsistencies in privacy complaint-handling agencies' investigative tools, the lack of coordination between the agencies, and issues identified by the Cyberspace Law and Policy Centre and ACCAN with respect to providing consistent, clear messages to consumers about their options.

---

35 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 50.

36 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 50.

37 M. Hummerston, Assistant Privacy Commissioner, media release, 14 September 2010.

Recommendation 1

2.31 The committee recommends that the government consider and respond to the recommendations in the Cyberspace Law and Policy Centre's report: *Communications privacy complaints: In search of the right path*, and recommendations from the Australian Communications Consumer Action Network arising from that report.

Industry self-regulation

2.32 Currently, because many organisations managing browsers, social networking sites, and other web 2.0 sites operate outside of the scope of the Privacy Act for various reasons,[38] the privacy of Australians online appears to be largely dependent on the policies and practices of the online sites they use.

2.33 For those Australian organisations that operate outside of the Privacy Act, while the OPC may issue guidelines for best practice in information handling and privacy policy, it is currently up to individual organisations to implement these policies. Overseas based organisations may be required to comply with privacy laws in the jurisdiction in which they are based.

2.34 With respect to organisations bound by the Privacy Act, the Act currently provides that organisations may develop industry codes with at least equivalent protections to the NPPs, which organisations within the industry may consent to be bound by. Codes must be approved by the Commissioner.[39] The government proposes to extend the powers of the Privacy Commissioner to request the development of an industry privacy code where the Commissioner considers it would be in the public interest for such a code to be developed.[40]

2.35 The government has also proposed that if an adequate code is not developed following such a request by the Commissioner, the Commissioner should have the power to develop and impose such a code following consultation with stakeholders.[41]

2.36 The OPC has suggested that binding codes may be appropriate:

> …for certain types of data-matching where there may be heightened privacy risks, for specific notice requirements for new technologies, and to allow standards developed by industry bodies to be given lawful effect.[42]

2.37 The OPC supports the government's proposal to expand its powers in this way, submitting that:

---

38 Predominantly because the organisations are based overseas or because they are Australian businesses subject to the small business exemption under the Privacy Act. The appropriateness of these 'exemptions' is discussed in Chapter 3.

39 *Privacy Act 1988*, s 18BB(2)(c).

40 Australian Government, *First stage response to ALRC Privacy Report*, 2009, recommendation 48-1, p. 89, www.dpmc.gov.au/privacy/reforms.cfm (accessed 13 September 2010).

41 Australian Government, *First stage response to ALRC Privacy Report*, 2009, recommendation 48-1, p. 89.

42 OPC, *Submission 16*, p. 12.

> Binding codes will allow greater flexibility in addressing privacy issues associated with new technologies or practices where industry has failed to effectively self-regulate and there is a compelling public interest in regulating these new practices or technologies…
>
> Such codes will allow the development of further detail on how the privacy principles apply in a particular circumstance. In this way, codes can provide specificity to the technology-neutral standards contained in the privacy principles.[43]

2.38 This approach was generally supported by consumer groups that appeared before the committee. Ms Teresa Corbin, CEO of ACCAN argued:

> Our general approach in relation to self-regulation [is], whilst we are happy for the industry to take initiatives and develop codes of practice that lift the bar and provide a model of best practice, we really do think that self-regulation has to be underpinned by a good regulatory framework in the first place, with the regulator having the ability to take strong enforcement action—not constantly, but when needed—and the power to do so when needed.[44]

2.39 However, organisations representing advertisers discussed the benefits of self-regulation and argued that it is currently working well. The Australian Association of National Advertisers (AANA) submitted that self-regulation is the best way to deal with privacy issues in online advertising, such as behavioural advertising, because of the speed at which technology changes.[45] The AANA submitted that self-regulation:

> …provides a flexible mechanism to meet the challenges of ever evolving advertising and marketing practices, media environment as well as consumer expectations.[46]

2.40 The AANA's CEO, Mr Scott McClellan argued that:

> A key benefit of this system is its ability to respond and adapt to evolving technology and changes in the way consumers access the media, both online and in the traditional sense. The AANA Code of Ethics, for example, is the overarching code for all Australian advertisers. It has the objective of ensuring that all advertising is ethical, and prepared with a proper sense of obligation to consumers and fairness to competitors.[47]

2.41 The AANA noted that it has had a self-regulatory framework since 1997 and has been proactive in addressing privacy issues. For example, the AANA submitted, that it has developed a code applying to marketing to children, which requires

---

43 OPC, *Submission 16*, p. 12.

44 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 49.

45 AANA, *Submission 3*, p. 2.

46 AANA, *Submission 3*, p. 4.

47 Mr Scott McClellan, CEO, Australian Association of National Advertisers, *Committee Hansard*, 29 October 2010, p. 27.

advertisers to obtain parental consent before disclosing the personal information of any child.[48] Mr McClellan informed the committee that the AANA Code of Ethics is currently under review. A final report and revised Code of Ethics was expected to be submitted to the AANA Board in late 2010; however the AANA has decided to postpone finalising it pending the outcome of a current House of Representatives committee inquiry into the regulation of billboard and outdoor advertising.[49]

2.42 Similarly, the Communications Council expressed support for self-regulation as an effective way of protecting privacy online. The Council submitted that it has already developed online privacy guidelines, which it states 'serve to increase trust between advertisers and consumers, and to foster the protection of consumer's privacy'.[50] The Council submitted that it is also in the process of developing voluntary codes and standards on online behavioural advertising and the privacy of children online.[51]

2.43 According to Yahoo!7, there are ongoing discussions and attempts within the industry to develop standards and best-practice approaches.[52] Yahoo!7 argued that there are benefits to allowing the industry to self-regulate to a significant degree:

> Most advances in online privacy protection have come as a result of industry initiatives undertaken to preserve user trust in the Internet medium, and through self-regulatory efforts that allow competitor companies to recognise consistent best practices that reinforce consistent user experiences online…Market forces encourage companies like Yahoo!7 to bring privacy innovations to our customers quickly.[53]

2.44 Google agreed with these sentiments, arguing that service providers have a motivation to provide a safe and secure online environment to users in order to retain users' trust. Google submitted:

> This is most true in the highly competitive world of the web, where an alternative is just a click away.[54]

2.45 Mr Flynn, Head of Public Policy and Government Affairs, Google Australia, argued:

---

48 AANA, *Submission 3*, pp 2–3.

49 AANA media release, 'AANA leads discussion on advertising and marketing ethics', 5 August 2010; Mr Scott McClellan, CEO, AANA, *Committee Hansard*, 29 October 2010, p. 30; Ms A. Bain, Director of Codes, Policy and Regulatory Affairs, AANA, House of Representatives Standing Committee on Social Policy and Legal Affairs, *Proof Committee Hansard*, 24 February 2011, p. 2.

50 Communications Council, *Submission 12*, p. 3.

51 Communications Council, *Submission 12*, p. 4.

52 Yahoo!7, *Submission 2*, p. 3.

53 Yahoo!7, *Submission 2*, p. 5.

54 Google, *Submission 6*, p. 1.

> Our view is that service providers generally, and certainly Google, want their services associated with comfort, safety and security, and ultimately that is imperative to the providers' bottom line. Otherwise, if we do not get that right, internet users will switch, and on the internet that is very easy. A different service is literally just a click away. That choice, that ability to switch, is a key protection for individuals. They can easily move to another service or two if they so choose.[55]

2.46 Mrs Rohan, Director, Corporate and Regulatory Affairs, Australian Direct Marketing Association (ADMA), expressed similar views with respect to regulating the use of behavioural advertising (discussed in detail in chapter 3):

> Privacy is good business. That means that, if consumers do not trust you or they are concerned about privacy, they will not deal with you. They will not give you the information and they will move to competitors.[56]

2.47 Mr Leesong, CEO, Communications Council, agreed:

> It cannot be understated how important the preservation of the brand is. In fact, if an agency does deliver a poorly executed campaign which is in breach of privacy principles or is pulled up, it can be fatal to that agency's business.[57]

2.48 However, despite these arguments that online industries have self-interest in providing adequate privacy protection, Mr McClellan, CEO, AANA, noted that the development of codes and self-regulatory guidelines has not been as widespread as might have been expected when the Privacy Act was developed.[58]

2.49 In response to a question about what the 'shelf life' of an industry's attempts to self-regulate ought to be, Mr Leesong, CEO, Communications Council stated:

> It is a bit 'how long is a piece of string'. Self-regulation has been around for a long time. From a regulator's perspective, it is reasonable to expect to see the industry being proactive and keeping its codes up-to-date. It is reasonable to expect the industry to be communicating its activities to people like yourself, to interested parties. I would not want to put a time frame on it, but it would be more 'actions speak louder than words'. If there was a real absence of communications and activities, then I think, quite rightly, the industry would be leaving itself open to being regulated.[59]

---

55 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 2.

56 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, Australian Direct Marketing Association, *Committee Hansard*, 29 October 2010, p. 53.

57 Mr Daniel Leesong, CEO, Communications Council, *Committee Hansard*, 29 October 2010, p. 40.

58 Mr Scott McClellan, CEO, ADMA, *Committee Hansard*, 29 October 2010, p. 28.

59 Mr Daniel Leesong, CEO, Communications Council, *Committee Hansard*, 29 October 2010, p. 40.

2.50 Mr McClellan seemed to agree that despite a preference for self-regulation, there may be scope for further regulation by OPC where self-regulation is insufficient:

> I think it would be an interesting thing to look at whether—in the context of reviewing privacy legislation and its provision for sectoral codes, as Timothy Pilgrim [the Privacy Commissioner] alluded to just a moment ago—there may be scope for more work in this area, to address the nuances of particular industry sectors and how they go to market.[60]

2.51 Mr McClellan also noted that the Privacy Act plays an important role in underpinning industry codes.[61]

Committee comment

2.52 The committee accepts that there can be significant benefits to self-regulation. The committee also accepts that there are strong incentives for some companies and industries, such as the online advertising industry, to develop strong privacy protection practices in order that customers feel secure in dealing with those organisations. However, the committee is not convinced that this is always the case. The discussion in chapter 3 of this report regarding behavioural advertising demonstrates that it is frequently very lucrative for organisations to sell personal information, which increases the self-interest in having lax privacy protections, or loopholes in privacy policy. Accordingly, the committee supports in-principle the government's proposal to strengthen the powers of the OPC to develop and enforce industry codes for specific industries which pose risks to the privacy of Australians.

Education

2.53 The OPC submitted that 'user-education will be critical to ensuring that individuals are equipped to protect their privacy online', because of the fact that 'many aspects of online privacy remain in the hands of the individual'.[62]

2.54 The Victorian Privacy Commissioner agreed:

> Ensuring that individuals are fully informed and able to understand both the benefits and risks inherent in online interaction and engagement will be, by far, the most effective and efficient method, whether they are engaging in social networking services or transacting online.[63]

2.55 The key way in which individuals are informed about the privacy implications of providing personal information online is through website privacy policies. The Privacy Act requires private sector organisations covered by the Act to publish privacy policies setting out the purposes for which personal information is being collected and the uses to which it may be put.[64] This theoretically allows users to

---

60 Mr Scott McClellan, CEO, AANA, *Committee Hansard*, 29 October 2010, p. 28.

61 Mr Scott McClellan, CEO, AANA, *Committee Hansard*, 29 October 2010, p. 28.

62 OPC, *Submission 16*, p. 17.

63 Victorian Privacy Commissioner, *Submission 13*, p. 9.

64 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

control their personal information by deciding whether or not to interact with an online organisation based on its stated privacy policies.

2.56 However, the Privacy Commissioner told the committee that:

> We hear constantly that privacy policies get extraordinarily complex and can become virtually worthless if people are not prepared to read them.[65]

2.57 The same point was made by a number of other witnesses that appeared before the committee.[66]

2.58 The committee heard about some best practice approaches, for example Google's use of videos to explain privacy features,[67] however to a large extent the complexity of a privacy policy and the quality of information available is dependent on the website operator.

2.59 Whilst acknowledging that at the end of the day, individual Internet users must inform themselves of what is going to happen to their information once they are online, the Privacy Commissioner advised the committee of the importance of finding new online privacy education approaches:

> So we have to find new mechanisms to allow people to understand what is going to happen to their personal information and be able to make educated choices before they enter into various transactions, or even when they are just browsing on the web—how do we educate the community? That is going to be one of the key areas.[68]

2.60 The OPC is empowered by the Privacy Act to undertake education programs in order to promote the protection of individual privacy.[69] In its review of Australian privacy law, the ALRC recommended that the OPC 'should develop and publish guidance in relation to technologies that impact on privacy',[70] which the government has indicated it supports.[71]

---

65 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

66 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 46; Ms Georgia King-Siem, Vice-President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 16; Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, Law Institute of Victoria (LIV), *Committee Hansard*, 1 December 2010, p. 31.

67 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 11.

68 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

69 *Privacy Act 1988*, para. 27(1)(m).

70 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, recommendation 10-3.

71 Australian Government, *First stage response to ALRC Privacy Report*, 2009, p. 31.

2.61 The OPC has already developed educational materials on various issues concerning cyber safety including on:

- privacy issues faced by young people;
- social networking and spam; and
- smartphones.

2.62 The ACMA has also developed a number of education programs relating to online privacy issues:

> Under the brand name of Cybersmart...the ACMA distributes a diverse suite of cybersafety and cybersecurity programs. These target young people and those who are best able to influence young people's online engagement such as parents, teachers, trainee teachers and librarians. Our goal is to ensure that Australians have the skills, tools and knowledge to engage in the digital economy fully with trust and confidence. We recognise that building messages about privacy and the protection of personal privacy into education programs is central to achieving this goal.[72]

2.63 The ACMA informed the committee of some of its recent privacy education campaigns which include:

- the 'Z-card': 'a credit card sized fold-out pamphlet containing tips on how consumers can increase the security and privacy of their mobile phones'; and
- 'for Valentine's Day this year we targeted users of online dating sites with a postcard promotion designed to help them protect their identity and personal information when interacting with others online'.[73]

2.64 However, some submitters argued that more could still be done. For example, Mr Arved von Brasch submitted that education about online privacy should be included in the school curriculum.[74]

2.65 Ms Nerida O'Loughlin, General Manager, ACMA, informed the committee that while it is not mandatory for students to be educated about online privacy:

> ...our experience is that there is a very strong focus in most schools these days on embedding cybersafety and cybersecurity issues as much as they can in their work programs. The materials that we offer also complement other materials offered such as the ThinkUKnow program...[75]

2.66 Dr Roger Clarke, Chair of the Australian Privacy Foundation (APF), argued:

---

72 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 56.

73 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 56.

74 Mr Arved von Brasch, *Submission 2*, p. 2.

75 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 57.

> Most real education that occurs is by peers...so it is about the kinds of features that are available and the way in which those features are used by the people seen by peers as being the smart ones—the leaders within the peer group. That is where the leadership needs to come from. That is why I stress this need for appropriate features in products, because if you make those features available then 'the street finds its uses for things'...[76]

2.67 In addition to educating the public about the privacy risks of providing personal information online, it is also important to educate those collecting and processing personal data. For example, the Community and Public Sector Union (CPSU) added that it is also important that public servants who received personal information that Australians have submitted online also need to be educated as to their obligations in both information sharing and privacy.[77]

2.68 Similarly, Mrs Melina Rohan, Director of Corporate and Regulatory Affairs, ADMA, discussed the importance of training advertisers about their privacy obligations, which is a service that ADMA provides:

> We provide compliance tools and websites. I teach a one-day compliance course 10 times a year. We have on call a 1-hour webinar which our marketers can access at any time. It highlights all of the requirements under the Privacy Act, the Do Not Call Register Act, the Spam Act, the Copyright Act and the Trade Practices Act.[78]

Privacy enhancing technology

2.69 The OPC submitted that technology may be configured to protect the privacy of individuals and limit the amount of information collected, for example by allowing individuals to remain anonymous, allowing websites to manage and obtain consent, or providing individuals with greater choice in relation to the secondary uses of their personal information.[79]

2.70 The committee received evidence from both Google and Yahoo!7 about their respective efforts to give users control over their privacy.

2.71 Google submitted that it takes privacy protection very seriously and has implemented a number of features which allow users to protect their privacy, including:

- *Google Dashboard* which allows users to control the privacy settings of their account;
- the ability for users to use 'incognito' mode in the *Chrome* browser, and to pause or delete their web history; and

---

76 Dr Roger Clarke, Chair, Australian Privacy Foundation, *Committee Hansard*, 1 December 2010, p. 12.

77 CPSU, *Submission 7*, p. 8.

78 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, ADMA, *Committee Hansard*, 29 October 2010, p. 58.

79 OPC, *Submission 16*, p. 18.

- encrypting *Gmail* by default.[80]

2.72 Yahoo!7 similarly submitted that it has voluntarily configured its sites to include privacy protections, including through:

> …easy navigation, information on special topics and [giving] prominence to our opt-out page, making it simple for users to find and exercise their privacy choices. We are also providing leadership in experimentation around ways to provide notice and transparency outside of standard privacy policies, thereby giving users multiple privacy touch points and greater insight into the ubiquity of data collection and its use online, notably around advertising.[81]

2.73 However, other witnesses argued that more could be done by companies like Google and Yahoo!7 to assist users in protecting their privacy. For example, Dr Clark, Chair, Australian Privacy Foundation (APF), argued that more facilities ought to be available to users who do not wish to log in and provide personal details.[82] Dr Clarke suggested that more would be achieved by meaningful and consultative discussion between major internet companies and public interest organisations, like APF.[83]

2.74 The OPC argued in its submission that:

> [W]hen privacy is 'designed into' new systems at a formative stage, those systems are more likely to protect and manage personal information effectively.[84]

2.75 The OPC suggested promoting these technologies in order to encourage their use and expand their availability and notes that the Canadian Office of the Privacy Commissioner allocates funding for non-profit research in the area.[85]

International Cooperation

2.76 One of the key difficulties with regulating online privacy results from the ease with which information can flow between jurisdictions. The OPC submitted that:

> Like other regulatory schemes, domestic privacy laws may struggle to cope with the ubiquitous nature of the internet.[86]

2.77 A number of international organisations have done work on this issue, developing various frameworks and making recommendations to member states.

2.78 For example, the Asia Pacific Economic Cooperation (APEC) adopted a Privacy Framework in 2004 which aims to encourage member states to develop

---

80 Google, *Submission 6*, p. 4.

81 Yahoo!7, *Submission 2*, p. 2.

82 Dr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 9.

83 Dr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, pp 10–11.

84 OPC, *Submission 16*, p. 18.

85 OPC, *Submission 16*, p. 19.

86 OPC, *Submission 16*, p. 19.

appropriate privacy protections.[87] The strength of the APEC framework was criticised by a number of organisations during the course of this inquiry, aspects of which are discussed further in chapter 3.[88]

2.79 The Data Privacy Subgroup of APEC has recently developed a 'multi-lateral cross-border privacy enforcement arrangement for privacy enforcement authorities'.[89] The arrangement allows participating authorities to assist each other in collecting evidence, sharing information on investigations, enforcing actions and transferring complaints across jurisdictions. Australia's OPC is a co-administrator of the arrangement and was closely involved with its development.[90]

2.80 The Organisation for Economic Cooperation and Development (OECD) also has a number of projects aimed at developing international privacy protection standards, with which Australia is involved. The OECD developed privacy guidelines in 1980 which provided the model for Australia's privacy laws.[91] Like APEC, the OECD also has a network through which privacy enforcement authorities cooperate—called the Global Privacy Enforcement Network.[92]

Appropriateness of Australia's multi-faceted approach

2.81 As noted above, the OPC submitted that Australia needs to take a multi-faceted approach to privacy protection, utilising a range of formal and informal mechanisms to protect the privacy of Australians online.[93] A number of submitters, including the Victorian Privacy Commissioner, AANA and Google expressed support for this approach.[94] Mr Flynn, Head of Public Policy and Government Affairs, Google Australia, commented:

> Our view is that the best policy approach to privacy combines education with carefully framed laws and with technology tools that put internet users in the driving seat.[95]

2.82 The committee broadly accepts these arguments. Legislation and enforcement mechanisms are clearly necessary to underpin any privacy regime. Yet, given

---

87 Available at www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html (accessed 22 October 2010).

88 See Cyberspace Law and Policy Centre, *Submission 26*; APF, *Supplementary Submission 14*, p. 10.

89 OPC, *Submission 16*, p. 20.

90 OPC, *Submission 16*, p. 20.

91 OPC, *Submission 16*, p. 20.

92 OPC, *Submission 16*, p. 20.

93 OPC, *Submission 16*, p. 10.

94 OPC, *Submission 16*; Victorian Privacy Commissioner, *Submission 13*; Australian Association of National Advertisers, *Submission 3*.

95 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 1.

jurisdictional boundaries and the transnational nature of the Internet, it would be impossible for legislation alone to adequately protect the privacy of Australians online, and accordingly it is clear that educational programs and international engagement must form part of any successful approach to privacy.

2.83 Furthermore, in many situations it will be more appropriate to allow the market to decide what aspects of privacy individuals are willing to forego in exchange for the convenience of, for example, not needing to re-enter personal details for every transaction. Self-regulation will have a key role in this regard in setting industry best-practice benchmarks.

2.84 However, as will be discussed in chapters 3 and 4, it is not clear that Australia's approach always strikes the right balance between the various facets of its privacy protection framework. There was some disagreement amongst submitters as to the appropriate balance between the various approaches. For example, Ms King-Siem, Vice President, Liberty Victoria, argued that the Privacy Act ought to be strengthened in various ways, and play a greater role underpinning Australia's privacy framework:

> We believe that privacy is a fundamental human right. It is recognised under article 17 of the [International Covenant on Civil and Political Rights]. We do not believe that it is adequately protected in Australia. There is what I would term a patchwork of legislative protections that we have. For instance, in our federal Privacy Act there is an exemption for small business. Small business is, going on the Victorian Privacy Commissioner's submission, approximately 95 per cent of business in Australia, which means that 95 per cent of business is not subject to privacy regulation. There are employee information exemptions. All this adds up to what we feel is a less than adequate privacy regime in Australia.[96]

2.85 Furthermore, in relation to a number of emerging issues, it seems Australia's current approach to privacy regulation is applying offline thinking to online situations. The committee cautions that, as online technology continues to develop and new privacy issues emerge, it will be necessary to continually evaluate Australia's privacy framework to ensure that regulators are not simply applying old policy values and frameworks, which may be well suited to the offline contexts, to a very different online situation.

2.86 As Mr McDonald, Board Member, Communications Council cautioned:

> [Applying offline thinking to online problems] is probably not just an industry problem but a nationwide problem. As consumers change their habits change. But we continually like to put things in boxes and the boxes do not always frame the question well and are not always able to answer the problem correctly. There is a need for more dynamic, out-of-the-box

96 Ms Georgia King-Siem, Vice President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 15.

thinking about some of these problems, and not just online but thinking about privacy. Clearly, it does not work when you apply it to Facebook.[97]

97 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, p. 41.

Chapter 3

Adequacy of Australia's online privacy framework

3.1 Rapid developments in online computing technology over recent decades have created important opportunities for Australian individuals and businesses, facilitating access to vast quantities of information and allowing businesses to take advantage of international markets. As Mr Flynn, Head of Public Policy and Government Affairs, Google Australia, noted:

> The online world offers tremendous opportunities for people—opportunities to get access to all the information in the world and opportunities to communicate and collaborate with people everywhere. Australians are enthusiastic users of the internet. We have research from Nielsen which shows that some 86 per cent of Australians have internet access.[1]

3.2 However, during this inquiry, it was emphasised to the committee that continuous advances in online technology and computing power creates constant challenges for privacy regulators around the world. The past decade has seen the development and rapid adoption of web 2.0 technologies—that is technologies 'characterised by enabling greater online interaction and user-generated content'[2] such as social networking websites, blogs and video and photo sharing websites—as well as rapid advances in computing power. These developments have made it possible to store and share great quantities of personal data, and made individuals increasingly likely to upload personal information onto the web.[3] A combination of these and other technological advancements has exacerbated existing concerns about the adequacy of Australia's privacy framework to protect the privacy of Australians online, as well as created new privacy concerns.

3.3 As the Privacy Commissioner, Mr Pilgrim explained:

> Privacy remains a key issue in the information age...In the internet age personal information is easy to access and publish. It is searchable, downloadable, reusable and can remain in circulation sometimes indefinitely.
>
> These changed conditions for information handling can have a significant impact on the protection of individual privacy. Once released online, it can be difficult to recoup, delete or control what happens to personal information.[4]

---

1 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 1.

2 OPC, *Submission 16*, p. 25.

3 OPC, *Submission 16*, pp 21-34.

4 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, pp 16–17.

3.4 Furthermore, the ease with which information can be sent overseas means that Australian regulators have a diminishing ability to control the way in which individuals and organisations capture, store and handle personal data. Ms King-Siem, Vice President, Liberty Victoria, noted:

> For almost any given interaction there is a good chance that your information is shooting its way around the world and some along the way may or may not be captured.[5]

3.5 Mr Jacobs, Chair, Electronic Frontiers Australia (EFA), explained that a key concern with personal data 'shooting its way around the world' and being captured is the uncertainty about whether the information is being monitored or stored, and if so, by whom and for what purpose:

> If your traffic is flowing through another country, for instance the United States, we have definitely heard reports about widespread real-time monitoring of communications in there. There was a lawsuit filed against AT&T for their complicity in installing massive hardware at the behest of the National Security Agency to monitor all of the real-time communications on AT&T's network, and that court case did not go anywhere because congress passed a law giving them retroactive immunity...when you send somebody an email, you do not know where it is going to go. It could certainly be in another jurisdiction where that [monitoring] is occurring...It is a public fact that information sent to China goes through the so-called 'great firewall', which does keyword monitoring, for instance.[6]

3.6 There have been a number of recent high profile instances of personal data being improperly captured or released. Possibly the most striking was the collection of payload data from unencrypted Wi-Fi networks by Google's street cars in over 30 countries, including Australia.[7] Representatives of Google who appeared before the committee described the collection as a 'mistake', as did Google's Senior Vice President of Engineering and Research.[8]

---

5 Ms Georgia King-Siem, Vice President, Liberty Victoria, *Committee Hansard*, 1December 2010, p. 22.

6 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 72.

7 See Fran Foo, 'Report shows Google collected Wi-Fi data', *The Australian*, 10 June 2010, www.theaustralian.com.au/australian-it/report-shows-google-collected-wi-fi-data/story-e6frgakx-1225877786307 (accessed 4 January 2011).

8 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 2; and the Official Google Blog, 'WiFi data collection: an update', 14 May 2010, at http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (accessed 4 January 2011).

3.7 Mr Flynn, Head of Public Policy and Government Affairs, Google Australia, stated that Google has apologised for this mistake, and taken steps to ensure similar privacy breaches do not occur in Google's future projects.[9]

3.8 While the Chair of EFA, Mr Jacobs, believes that 'Google should have known better and should have done better', and that Google 'deserve[s] to cop a bit of flack for what they did, because it was a serious invasion of privacy'[10], Mr Jacobs also acknowledged that the incident was most likely an error rather than a deliberate 'part of a broader or more sinister trend to spy on people'.[11]

3.9 The committee notes that the AFP has finalised its investigation into whether Google's actions constituted a breach of the *Telecommunications (Interception and Access) Act 1979*, finding that while there may have been a breach, it was inadvertent. In addition, the AFP concluded that the difficulty in gathering evidence means that pursuing the matter further 'would not be an efficient and effective use of the AFP's resources'.[12]

3.10 Another recent, high profile example involved applications on the social networking site, Facebook, transmitting personal information to advertising companies without user's knowledge or consent, and against Facebook's privacy policy.[13]

3.11 The implications of these privacy breaches for individuals can be significant. Criminals can aggregate online personal data to facilitate criminal activity, such as identity theft and fraud.[14] Concerns have also been raised that the aggregation of data may leave certain groups of individuals vulnerable to discrimination. For example, the Australian Federation of AIDS Organisations submitted that without careful data privacy controls, the aggregation of health records may result in HIV-positive individuals being discriminated against by health providers because of their HIV-positive status.[15]

3.12 Individuals whose personal data is released can also, and probably more commonly, suffer great embarrassment as a result of the information being publicised,

---

9 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 2.

10 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 67.

11 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 67.

12 AFP, *Media Release: Finalisation of Google referral*, 3 December 2010, at www.afp.gov.au/media-centre/news/afp/2010/december/finalisation-of-google-referral.aspx (accessed 19 January 2011).

13 Emily Steel and Geoffrey Fowler, 'Facebook in privacy breach', *The Wall Street Journal*, 18 October 2010, at http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html (accessed 4 January 2011).

14 Mr Alastair MacGibbon, Internet Safety Institute, *Submission 8*, p. 5.

15 Australian Federation of AIDS Organisations, *Submission 23*, p. 3.

or further intrusions on their privacy such as unsolicited emails or telephone calls from marketers.

3.13 The CEO of the Australian Communications Consumer Action Network (ACCAN), the peak body for Australian consumers on telecommunications and online issues, Ms Corbin, told the committee that:

> Our membership, and consumers in Australia generally, highlight that they are very concerned about privacy issues overall, especially given the greater reliance upon communications technology and also by companies who collect our personal data on technology that includes access to cloud applications and databases that are perhaps increasingly collecting more and more information with a potential for harm and for mistakes to happen increasing in magnitude as a result.[16]

3.14 During this inquiry the committee received evidence about a large number and wide range of privacy concerns that have been created or exacerbated by online technological advances. It is not practical for the committee to explore all of the concerns raised in detail in this report. Instead, this chapter has identified five key aspects of Australian privacy framework which underpin the vast majority of concerns raised during this inquiry about the adequacy of protections for the privacy of Australians online:

- consent;
- the exemption of small businesses from the *Privacy Act 1988*;
- online behavioural advertising;
- transnational data flows; and
- whether Australia needs a statutory cause of action for breach of privacy.

Consent

3.15 The Australian Privacy Foundation (APF) submitted that:

> The concept of consent is probably the single most serious weakness in Australia's privacy regulation. No matter how dire, there is virtually no type of privacy violation that cannot be justified by reference to the victim having consented to the action in question.[17]

3.16 Many of the restrictions on the collection, use and disclosure of personal information that apply under the Privacy Act can be avoided if an individual's consent is obtained. For example restrictions apply on the use of information for a secondary purpose (i.e. not the purpose for which it was collected), and the transfer of information offshore under a contract. However the restrictions do not apply if consent is obtained.[18] The exposure draft of the new APPs retains the centrality of

16 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, pp 33–34.

17 APF, *Submission 14*, p. 2.

18 *Privacy Act 1988*, Schedule 3, NPP 2 (use for a secondary purpose), and NPP 9 (transborder data flows).

consent in overcoming many of the restrictions placed on the collection, use and disclosure of personal information.[19]

3.17 The APF argued that the ease with which consent can be obtained is disproportionate to the cure-all effect that it has on individual privacy, and commented:

> Privacy protection is virtually meaningless where its protective application can be so easily circumvented, for example by [an] Internet user being forced to "consent" to unspecific privacy invasive practices, bundled with pages of other terms and conditions, when signing up for a social networking account.[20]

3.18 The APF suggested that stricter regulation of consent is required, and suggested consumer protection measures of the *Trade Practices Act 1974* as a model.[21]

3.19 As briefly discussed in chapter 2, the privacy policies to which individuals are often required to consent in order to obtain an online service are often lengthy and complex. This issue was raised by a number of submitters and witnesses to this inquiry.[22]

3.20 Ms Corbin, CEO, ACCAN, informed the committee that:

> Most consumers tell us that they do not read them [privacy statements] and that they just tick a box because they want to get on and use the service...In the end people really want to use the services, so they are faced with the decision of whether to use the service or to waive a right, and in most instances they do not understand the legalese that they are waiving their right to. So it is ultimately a waste of time to have these agreements.[23]

3.21 Similarly, Ms Miller, from the Law Institute of Victoria, stated:

> I think with online access everyone wants it to be quick and is used to it being quick. When confronted with a 20-page document that still seems to

---

19 See for example draft APP 3 (relating to collection of sensitive information); APP6 (relating to the use of information for a secondary purpose); APP 7 (direct marketing); and APP 8 (relating to transborder data flows).

20 APF, *Submission 14*, p. 2.

21 Section 51AB of the *Trade Practices Act 1974* relates to corporations acting in a way which is unconscionable in their dealings with consumers. Relevant factors include the relative strengths and bargaining positions of the parties, the consumer's knowledge and understanding, and the exertion of undue pressure or influence.

22 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22; Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 47; Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 16; Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 31.

23 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 47.

> be written in 1950s legalese and which has not been touched by the trend towards plain English, I absolutely agree that people just click through.[24]

3.22 Ms King-Siem, Vice President, Liberty Victoria, agreed with the APF's submission about the idea of consent being 'a bit of a furphy',[25] because of the fact that people are required to tick a box waiving their legal rights so that a transaction can occur.[26] Ms King-Siem argued that much of the time the personal information collected as a result of this 'consent' or waiver is not even necessary, and gave the example of Facebook requiring users to enter their real name.[27]

3.23 However, Mrs Rohan, Director, Corporate and Regulatory Affairs, ADMA, disagreed, arguing:

> The majority of websites have pretty clear privacy statements. In addition to that, they have very clear cookie statements. It is difficult to see how they would be manipulating people in those instances.[28]

3.24 Mrs Rohan used the example of a recent lecture at which she asked advertising students whether they played games on Facebook, and received the response that many did not because they had read the privacy policies and decided against using those services.[29] Mrs Rohan stated:

> The issues that ACCAN raised of some people not understanding the privacy policies and the readability and the understandability of them are true, but I do not think that should denigrate the fact that a vast amount of the population are alert to potential privacy issues, do read consent notices or privacy notices and do make a choice not to deal in some instances where they have concerns.[30]

Committee comment

3.25 The committee agrees with the comments of most witnesses, including the Privacy Commissioner, about the fact that people are often required to consent to numerous pages of legalese, waiving their privacy rights, in order to use web-based

---

24 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 32.

25 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 16.

26 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 19.

27 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 16.

28 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, Australian Direct Marketing Association, *Committee Hansard*, 29 October 2010, p. 57.

29 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, ADMA *Committee Hansard*, 29 October 2010, p. 54.

30 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, ADMA, *Committee Hansard*, 29 October 2010, p. 54.

services. Anecdotal evidence indicates that most consumers simply 'tick and flick' these consent forms without actually reading them. In the committee's view this is a serious problem that needs to be addressed within Australia's privacy framework.

3.26 While the Privacy Act has long allowed consent to justify the waiver of privacy rights in the offline sphere, it seems to the committee that the over-use of complex consent forms has increased exponentially with the expansion of online services. Furthermore, Liberty Victoria submitted that offline and online transactions requiring consent have some fundamental differences, namely that:

- online transactions often are not covered by Australian law;
- the data may therefore be used for purposes, or disclosed to other organisations, not envisaged by the consumer;
- third parties may be collecting the transactional data; and
- electronic data is rarely deleted, and is more accessible to more people and organisations than offline data.[31]

3.27 Liberty Victoria also argued that:

> Social and financial pressure is increasing on consumers/businesses to interact online. Goods are cheaper, bills lower when paid online and social networking sites have reached ubiquitous levels; the pressure to interact/transact online has increased, but the understanding of that transaction/interaction has decreased. In practice, this lack of knowledge reduces the 'genuineness' of consent in online transactions/interactions.[32]

3.28 The United States Federal Trade Commission (FTC) recently reported on 'Protecting Consumer Privacy in an Era of Rapid Change' and recommended a framework for businesses and policymakers in dealing with consumer privacy issues.[33] The FTC's findings corroborated the Australian Privacy Commissioner's evidence that privacy notices are often ineffective, misconstrued by consumers, lengthy and unclear.[34] The FTC recommended that:

> Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.[35]

---

31 Liberty Victoria, answer to question on notice, 1 December 2010.

32 Liberty Victoria, answer to question on notice, 1 December 2010.

33 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010.

34 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, pp 70–71.

35 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 70.

3.29 Based on the evidence received in this inquiry, the committee wholeheartedly supports this recommendation of the FTC in the Australian context. The committee also emphasises the importance of an enforcement mechanism to ensure that industry complies with a requirement for shorter, clearer and more standardised privacy notices. Accordingly, the committee urges that the Privacy Commissioner's complaint-handling role under paragraph 21(1)(ab) of the Privacy Act be expanded to more effectively address complaints about the misuse of consent forms in the online context, particularly those which result in the disclosure of personal information. The committee also recommends that the OPC consider the issue of the genuineness of consent in the online context, and develop guidelines on the appropriate use of privacy consent forms for online services.

Recommendation 2

3.30 The committee recommends that the Australian Privacy Commissioner's complaint-handling role under paragraph 21(1)(ab) of the Privacy Act be expanded to more effectively address complaints about the misuse of privacy consent forms in the online context.

3.31 The committee further recommends that the Office of the Privacy Commissioner examine the issue of consent in the online context and develop guidelines on the appropriate use of privacy consent forms for online services.

Small Business exemption

3.32 Since amendments made in 2000, the vast majority of Australian businesses have been exempt from complying with the requirements of the *Privacy Act 1988*.[36] The Act provides that small businesses are excluded from the definition of 'organisation' under the Act and are generally exempt from its operation.[37] A small business is defined as having an annual turnover of $3 million or less.[38]

3.33 However, a small business may be captured by the Act if it:

- provides health services and holds health information (other than employee records);[39]
- collects personal information or discloses personal information for a benefit, service or advantage (unless it always has the consent of the individuals concerned or always does so when authorised by legislation);[40]
- is providing services to the Australian Government or its agencies;[41]
- is related to a larger business;[42]

---

36 *Privacy Amendment (Private Sector) Act 2000*.

37 *Privacy Act 1988*, s. 6C.

38 *Privacy Act 1988*, ss. 6D(1).

39 *Privacy Act 1988*, para. 6D(4)(b).

40 *Privacy Act 1988*, para. 6D(4)(c) and (d); ss. 6D(7) and (8).

41 *Privacy Act 1988*, para. 6D(4)(e).

- is a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*;[43]
- is a 'protected action ballot agent', or an association of employees for the purposes of the *Fair Work Act 2009*;[44]
- is prescribed by regulation;[45] or
- opts in to the Act.[46]

3.34 While the committee was not provided with recent, official data on the number of small businesses with annual turnovers of $3 million or less, as at June 2007, 94 per cent of actively trading businesses in Australia had annual turnovers of less than $2 million.[47] Accordingly, the Act's small business exemption applies to the vast majority of Australian businesses, including most of those that collect personal information online.

3.35 The Privacy Commissioner, Mr Pilgrim, explained to the committee:

> If an organisation within Australia is a small business, as defined by the Privacy Act—that generally means it falls underneath the $3 million threshold—then the Privacy Act does not apply to any of its activities: how it collects the information, what it needs to do with the information, and who it passes it on to. Flowing from that scenario, if that small business that is exempt from the act then passes that information to an organisation overseas, and assuming that that organisation overseas has no links to Australia, then with that scenario the Privacy Act would not come into play for either the small business or the overseas entity, and therefore that personal information would not be subject to the protections of the Privacy Act.[48]

3.36 The purpose of amending the Act to exempt most small businesses was 'to minimise compliance costs for small businesses'.[49] The (then) government also justified the exemption on the basis that many do not pose a high risk to privacy.[50]

---

42 *Privacy Act 1988*, ss. 6D(9).

43 *Privacy Act* 1988, ss. 6E(1A); *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, s. 5.

44 *Privacy Act 1988*, ss. 6E(1B) and (1C).

45 *Privacy Act 1988*, ss. 6E(1) and (2); for example, regulation 3AA of the *Privacy (Private Sector) Regulations 2001* provides that small businesses that operate residential tenancy databases are organisations for the purposes of the *Privacy Act 1988*.

46 *Privacy Act 1988*, s. 6EA.

47 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108, May 2008, Chapter 39, citing Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), p. 20.

48 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

49 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000, pp 37–38.

3.37 In 2005, the Senate Legal and Constitutional Affairs References Committee considered the exemption, and recommended that it be removed from the Act, given that the exemption is 'too broad and too complex', that 'privacy rights should not disappear just because a consumer happens to be dealing with a small company', and the fact that 'other jurisdictions, such as New Zealand, operate effectively without any small business exemption'.[51]

3.38 In its review of the Act in 2008, the ALRC found that 'given the increasing use of technology by small businesses, the risk posed to privacy may not necessarily be low'.[52] Accordingly, the ALRC also recommended that the small businesses exemption be removed from the Act.[53] The government has not yet responded to this particular recommendation.

3.39 Mr Pilgrim, the Privacy Commissioner, argued that there needs to be a balance between ensuring that small businesses are not overly and unnecessarily burdened by privacy regulation and ensuring that those businesses with large holdings of personal information are required to protect that information.[54] Mr Pilgrim discussed Internet Service Providers (ISPs) as an example of a business that might hold large quantities of personal information about customers but which might have an annual turnover of under $3 million and thus be exempt from the Privacy Act.[55]

3.40 Mr Pilgrim informed the committee that:

> There is already provision within the Privacy Act that, in that situation, a group of organisations such as ISPs can be inscribed into the coverage of the Privacy Act—so there is a mechanism to do that.[56]

3.41 The provision to which Mr Pilgrim referred provides that regulations may prescribe that the Act applies to a class of small business operators which would otherwise be classified as small businesses.[57]

3.42 Mr Pilgrim warned:

> We would need to look carefully at any recommendation to remove the small business exemption, because I too would acknowledge that there is potentially an impost through the regulatory process on small businesses

---

50 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000, pp 37–38.

51 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, p. 157.

52 ALRC Report 108, 2008, paragraph 39.143.

53 ALRC Report 108, 2008, recommendation 39-1.

54 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, pp 19–20.

55 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 20.

56 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 20.

57 *Privacy Act 1988*, ss. 6E(1).

> that may not need to have that sort of impost. If I could use not a glib term but a colloquial example: the local fish and chip shop or the corner milk bar may have very little personal information. But if you remove a blanket exemption like the Privacy Act from small business then there may be issues that they would have to consider that may not necessarily warrant that level of regulatory burden on them.[58]

Committee comment

3.43 The committee notes that the exemption of small businesses from the Privacy Act means that over 90 per cent of Australian businesses are currently not required to comply with the provisions of the Act. This is entirely appropriate for many traditional offline businesses, such as a local fish and chip shop, in which limited details about customers are given during a transaction, and accordingly the business's holdings of personal customer information are likely to be limited and its risk to privacy low.

3.44 However, the exponential growth in the use of online technologies through which consumers transact and interact with business means that a growing number of small Australian businesses may now hold and use significant quantities of personal information which is routinely given in the course of an ordinary online transaction.

3.45 Furthermore, there are new categories of companies which operate in the online environment and by their nature have access to vast quantities of personal data, such as ISPs.

3.46 In other words, the online business environment in which many small Australian businesses now operate appears to present substantially greater risks to personal privacy than the old offline model.

3.47 The committee is particularly concerned about the fact that certain small businesses which hold significant quantities of personal data are exempt from the Privacy Act and accordingly are able to transfer the personal information of their customers offshore without restriction or oversight. In the committee's view, small businesses which hold significant quantities of personal information, or which transfer personal information offshore, ought to be subject to the provisions of the Privacy Act.

3.48 The committee accepts the Privacy Commissioner's comments about there being existing mechanisms within the Privacy Act through which categories of small business that pose a significant risk to privacy can be made subject to the Act through prescription in regulation. However, the committee believes that these existing mechanisms must be utilised more effectively by government. It would be timely and appropriate for the Privacy Commissioner to conduct a review of categories of small businesses with significant holdings of personal information and to make recommendations to government regarding the prescription of additional categories of small businesses which ought to be subject to the requirements of the Privacy Act. The government must ensure that the risks posed to individual privacy by small

58 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 20.

businesses which routinely hold significant quantities of personal data or which transfer personal data offshore are mitigated by Australia's privacy framework.

3.49 Proposed Australian Privacy Principle 8 has provisions relating to transfer of information overseas; however the small business exemptions will still apply. In the committee's view all organisations transferring personal information overseas should be subject to the Privacy Act.

Recommendation 3

3.50 The committee recommends that the small business exemptions should be amended to ensure that small businesses which hold substantial quantities of personal information, or which transfer personal information offshore are subject to the requirements of the *Privacy Act 1988*.

3.51 To achieve this end, the committee urges the Australian Privacy Commissioner to undertake a review of those categories of small business with significant personal data holdings, and to make recommendations to government about expanding the categories of small business operators prescribed in regulations as subject to the *Privacy Act 1988*.

3.52 The committee further recommends that the second tranche of reforms to the *Privacy Act 1988* amend the Act to provide that all Australian organisations which transfer personal information overseas, including small businesses, must ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.

3.53 Related discussion relevant to small business transferring personal information overseas is at paragraph 3.106ff.

Online behavioural advertising

3.54 Developments in online technology have created new, lucrative opportunities for advertisers. In its submission, the Internet Safety Institute described online businesses which have 'made enormous profits by "monetising" personal data' through online behavioural advertising.[59]

3.55 There are a number of ways in which web service providers are now able to collect data about individuals which is incredibly useful for the purposes of targeted, or behavioural advertising. For example, the amount of personal information that individuals upload on social networking sites—such as age, location, hobbies and interests—means that the operators of those sites have a huge range of personal data that is very useful to advertisers. Mr Jacobs, Chair, EFA, explained:

> If you are an advertiser and you go to Facebook, you can place an ad that only goes to university students between the ages of 18 and 23 who are interested in horses but are not yet members of the Equestrian Federation of Australia, for instance. From an advertiser's point of view that is a goldmine and you would be willing to pay a very high premium to target an advertisement that way, as opposed to something that is just seen by

59 Internet Safety Institution, *Submission 8*, p. 4.

> everybody. The more niche your market is, then the more you are willing to pay.[60]

3.56 Another 'goldmine' for advertisers is the ability of search engines to track a user's web browsing history. Google Australia, for example, informed the committee that it routinely holds browser history linked to an IP (Internet Protocol) address for nine months.[61] This information could be used to compile statistics and to analyse consumer behaviour for the purposes of targeted marketing.

3.57 A further technique that is widely used is the placement of 'cookies'—a text file stored by a web browser when a user visits a particular website, which then sends messages back to the server each time the user requests that page.[62] Representatives from Google Australia explained how cookies are used for behavioural advertising:

> The interest based advertising system effectively uses a cookie and, when the machine on which that cookie is present visits one of those websites, that is added to what we have as an anonymous database. Over time that may effectively add interest categories. For example, if a particular machine is visiting a lot of sports websites, then over time the interest based advertising system will conclude that that particular user is interested in ads for sports. Then, when that user goes to another website on that broad Google Display Network, they may get an ad for sporting material.[63]

3.58 Providers of web-based email services are also able to filter the content of users' emails, searching for key words, and advertise based on the content of an email. Ms Vij, Manager, Public Policy and Government Affairs, Google Australia, explained:

> It is the same kind of technology that also scans to identify viruses or spam. In a similar way it looks for particular word—or patterns, I guess, in the case of viruses or spam—to identify that, in the case of advertising, this keyword appears, so this might be a relevant ad. If a person does not want to see advertising on Gmail they can use the HTML version of Gmail.[64]

3.59 The Attorney-General's Department advised the committee that there is nothing to prevent web-based email service providers filtering emails in such a manner under Australia's telecommunications interception legislation, because of the fact that users agree to the filtering when they sign up to the email service.[65]

---

60 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 63.

61 Ms Ishtar Vij, Manager, Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 4.

62 www.webopedia.com (accessed 6 January 2011).

63 Mr Iarla Flynn, Head, Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 10.

64 *Committee Hansard*, 29 October 2010, p. 14.

65 Attorney-General's Department, answer to question on notice, 29 October 2010.

3.60 A number of witnesses and submitters also discussed the advertising opportunities that will be created with the advent of location based social networking services. Mr McDonald, Board Member, Communications Council, commented that:

> If you have subscribed to a service like Foursquare, it allows you to broadcast to your social network where you are—Facebook does the same now. The advertising model on Foursquare is to give local deals...Obviously with location based services for the consumer it is incredibly important to be relevant. If I am in a shopping centre—I think it is great to use shopping centres as an example—and I am shopping for the best deal, advertisers are in a situation where those types of services can enable their products to be found and the consumers at that point are given more choice.[66]

3.61 As a result of all of these ways that web service providers are now able to collect personal information about users of their services, advertising has become increasingly targeted to an individual's interests and location. Privacy Commissioner, Mr Pilgrim, observed:

> What we are dealing with here in terms of marketing is that, when you or I go on the internet—whatever we are doing—we will get advertisements coming up to us. As you say, those advertisements are getting more and more targeted because of the ability of the systems to be able to check our browsing history, look at our IP address and make assumptions that the person at the other end is interested in something. [67]

3.62 As outlined below, representatives of the advertising industry argued that these forms of targeted marketing are in both advertisers' and consumers' interests.

3.63 However, a number of witnesses and submitters expressed concern about the level of monitoring that these technologies now allow.[68] The Privacy Commissioner argued:

> In my view individuals should be able to move about the web without their movements being tracked or monitored by others, including the providers of targeted advertising.[69]

3.64 Currently, NPP 2 of the Privacy Act allows the use of personal information in targeted advertising provided certain conditions are met: it is impracticable to obtain consent; the individual has not made a request not to receive direct marketing; the

---

66 Mr Iain McDonald, Board Member, The Communications Council, *Committee Hansard*, 29 October 2010, p. 42.

67 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

68 See for example Internet Safety Institute, *Submission 8*, pp 4–5; Pirate Party Australia, *Submission 4*, p. 4; Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, pp 69–70; and Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 21.

69 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 18.

individual is informed in each communication of their ability to request the marketing to stop and will not be charged for this; and each communication sets out the organisation's address and telephone number.[70]

3.65 NPP 2 distinguishes between information collected for the primary purpose of advertising and information collected for another purpose. Draft amendments to the Privacy Act, released by the government in June 2010, intend to impose an alternative distinction between individuals who have provided personal information to the advertiser and those who have not.[71] However the Privacy Act does not and will not apply to behavioural advertising if the information gathered is not 'personal information'.[72]

3.66 Users of these advertising technique argued that the information about browsing history cannot identify an individual, and therefore cannot be defined as personal information under the Privacy Act.[73] However, the OPC submitted that:

> Over time, however, the aggregation of data may enable identification of individuals. When America Online released three months' search terms in 2006, for instance, it proved possible to identify individual users.[74]

3.67 Ms King-Siem, Vice President, Liberty Victoria, agreed:

> If you take what would be alleged to be an anonymous web user's browsing history but if you only have one person living at a particular address then that effectively means that that is personal information because it is identifiable or ascribable to a particular person. It is a very convenient way to say that it is actually anonymous data when, by the nature of where it has come from or other relevant factors, it is easy to determine who it actually belongs to. That point, strictly speaking, is when it becomes personal information. Before that point it is not, even though all the tools are at hand to make it personal information.[75]

3.68 Mr McDonald, Board Member, Communications Council, and founder of a digital advertising agency, disagreed, arguing that behavioural advertising is more akin to advertising at a sporting event:

> To a large extent when we are firing behavioural advertising it is just the same as going to a football match and knowing that there are many people there who like sport. We do not target individuals. It is very, very difficult. Even if we wanted to, the data is not there for us to do that. Certainly

---

70 *Privacy Act 1988*, Schedule 3, NPP 2.1.

71 Australian Privacy Principles, Exposure Draft, APP 7 available at www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/guide/exposure_draft.pdf (accessed 28 September 2010).

72 OPC, *Submission 16*, p. 29.

73 See for example Yahoo!7, *Submission 2*, p. 3.

74 OPC, *Submission 16*, p. 29.

75 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 21.

> Google et cetera do a pretty good job of disallowing that type of activity. If I were talking about personal data specifically, I think Facebook would be the biggest concern because we are able to advertise things that you like based on what is in your profile. Then again, you have the freedom of information to turn on what you like and what you do not like. But certainly there is a lot of development in that area and we are very careful around how we use that.[76]

3.69 Mr McDonald further stated:

> In terms of tracking and tracing, it is really not something where the agencies themselves have that data. That data is held by the social networks or maybe by the manufacturers themselves. To my knowledge, we have not seen the opportunity to use specific data other than targeted to a location, not a person.[77]

3.70 Google supported this evidence, and informed the committee that it places great importance on individual privacy concerns, and accordingly will not provide web browser history directly to advertisers.[78]

3.71 Advertisers argued that not only do these modern advertising data collection techniques assist advertisers in targeting their audience, they also benefit web users. For example, Mr Leesong, CEO, Communications Council, argued that:

> Consumers do have a level of comfort in knowing that the communication is targeted towards their specific interests. If I have an interest in computers, I would much rather be reading about the latest software rather than reading about the latest widget manufacturers.[79]

3.72 Mr McDonald, agreed:

> We know from all the studies that we have done that more effective advertising leads to greater consumer love or trust for a site, and certainly contextual advertising, from point to view of being relevant, deeply affects the experience around the site...Whenever we run a campaign, we might see that a banner ad is or is not being clicked on et cetera. There is a lot of analysis that goes into looking at not just effectiveness but also how much a consumer has actually enjoyed an experience. It is a very important part of the journey.[80]

---

76 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, p. 36.

77 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, p. 42.

78 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 11

79 Mr Daniel Leesong, CEO, Communications Council, *Committee Hansard*, 29 October 2010, p. 36.

80 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, p. 36.

3.73 Mr McDonald also pointed out that the targeted advertising enabled by these techniques also has the benefit of allowing advertisers to ensure that ads are not inappropriately targeted, for example to minors:

> If we want to protect the younger audience, then we are able to use the same systems to make sure that advertising reaches the right audience—the right products that do not offend different people.[81]

3.74 Mr McDonald continued:

> ...you could even look at it from the perspective that the same technology could be used to target people who were in areas prone to bushfires so that they receive the messaging, as opposed to people who were not in those affected areas. So there is a lot of good that comes out of this technology, and I think as an industry we try to find the best way to utilise those technologies for good...[82]

3.75 The AANA also emphasised that advertising plays an important role for Australian businesses in informing consumers about their choices and driving business.[83]

Regulatory options

3.76 In response to concerns about the perceived intrusiveness of individuals' online behaviour being monitored, the Privacy Commissioner expressed the view that:

> What we would like to see as much as possible in that context is choice—choice for the individual to know what is happening and choice to be able to at least opt out if not opt in to that sort of marketing, where it is effective and will work.[84]

3.77 Google submitted that its users do have such choice, through their *Dashboard* feature. However, the committee notes the comment of Mr Jacobs, Chair, EEFA, that 'only a very sophisticated user can manage all of this'.[85]

3.78 Given the previously discussed difficulties with respect to the complexity and length of many privacy policies, the committee explored the possibility of an opt-in model for web users to agree to receive behavioural marketing based on their web browser history and other personal data. Mr Flynn, Google Australia's Head of Public Policy and Government Affairs, argued that:

> Advertising is one of the key ways that pays for all the services that people can access online. Internet users have become used to the ability to freely

---

81 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, p. 36.

82 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, pp 36–37.

83 AANA, *Submission 3*, p. 2.

84 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

85 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 70.

> access a lot of very useful information. Interest based advertising is generally about trying to make advertising more useful and about trying to allow, in particular, publishers, news organisations and others to get a better revenue stream. One of the big challenges in the internet space that we face is making good content pay for itself. So a system that requires 'opt in' could have a negative impact, but I do not want to speculate beyond that because obviously there would be complex legal and operational questions.[86]

3.79 Mr Jacobs, Chair, EFA, expressed a similar view:

> Being able to show somebody who is reading an email about the Bahamas an advertisement for a trip to the Bahamas has enormous value for the advertisers and for Google. Therefore it is not in their interests to put up an opt-in model. There is no technological reason why it could not be opt in, but there is a very compelling—from Google's case—business reason, and that is the pressure that we are always going to be dealing with.[87]

3.80 As a result of its recent inquiry into 'Protecting Consumer Privacy in an Era of Rapid Change', the United States Federal Trade Commission recommended that a 'Do Not Track' mechanism for online behavioural advertising be developed.[88] The FTC in its investigation found that 'companies engaged in behavioural advertising may be invisible to most consumers'.[89]

3.81 The FTC has encouraged the development of tools to allow consumers to control and manage the information collected about them online, and noted in its report that some organisations have responded by developing such tools. The FTC noted Google's ad preferences manager and Yahoo!'s ad interest manager as examples. The FTC also noted the development of self-regulatory guidelines by an industry group comprised of media and marketing associations.[90]

3.82 However, the FTC found that despite these developments 'an effective mechanism [to improve consumer control of behavioural marketing] has yet to be

---

86 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 11.

87 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 210, p. 71.

88 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 63.

89 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 64.

90 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 64.

implemented on an industry-wide basis'.[91] The report noted that the use of existing mechanisms is low as consumers are often unaware of them.[92]

3.83 Accordingly, the FTC recommended that a 'Do Not Track' mechanism be established to 'support a more uniform and comprehensive consumer choice mechanism for behavioural advertising'.[93] In terms of enforcement, the FTC noted that the 'Do Not Track' mechanism could be established either by legislation or 'potentially through robust, enforceable self-regulation'.[94] In terms of implementation, the FTC suggested:

> ...placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements.[95]

3.84 The committee notes that there is currently an industry-wide initiative in Australia to develop standards for privacy regarding online behavioural advertising. A cross industry group of marketing and advertising industry bodies—including ADMA, AANA, the Communications Council, the Internet Industry Association, the Media Federation of Australia and the Interactive Advertising Bureau—was formed in November 2010 to develop the guidelines.[96] The committee notes the industry's stated commitment to developing online behavioural advertising standards including its pledge to 'share these guidelines with the Senate Committee and the industry as a whole as soon as practicable'.[97] The group released its guidelines in March 2011. The guidelines provide, amongst other things, that:

---

91 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 64.

92 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 65.

93 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 66.

94 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 66.

95 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010, p. 66.

96 *Media Release: Cross Industry Group to establish standards for online behavioural advertising in Australia*, 26 November 2010, at www.aana.com.au/documents/01-CrossIndustryGroupformstoestablishstandardsFINAL.pdf (accessed 19 January 2010).

97 *Media Release: Cross Industry Group to establish standards for online behavioural advertising in Australia*, 26 November 2010.

- Service Providers should obtain Explicit Consent prior to engaging in Third Party online behavioural advertising (OBA); and
- Service Providers should provide an easy to use mechanism for Web Users to withdraw their Explicit Consent to the collection and use of OBA Data for Third Party OBA.[98]

Committee comment

3.85 The committee strongly supports the recommendation of the FTC regarding the need for a more effective mechanism through which consumers can choose and manage their behavioural marketing preferences. Noting the ongoing industry initiative to develop self-regulatory standards on online behavioural marketing, the committee strongly commends the proposed US model to industry.

Recommendation 4

3.86 The Committee recommends that the OPC in consultation with web browser developers, ISPs and the advertising industry, should, in accordance with proposed amendments to the Privacy Act, develop and impose a code which includes a 'Do Not Track' model following consultation with stakeholders.

Transnational information flows

3.87 One of the major obstacles to the Australian government effectively regulating online privacy is the transnational nature of the internet. The Australian Parliament is only able to enact privacy laws relating to companies incorporated in Australia or with an Australian link, and it is increasingly easy for organisations to relocate around the world to a jurisdiction with the most favourable laws for its operation. This makes international cooperation a key component of any effective privacy protection framework. As Ms King-Siem, Vice President, Liberty Victoria explained:

> Even if we have the strongest privacy laws in the world, if we cannot enforce them it does not do us much good. That is where international cooperation is key.[99]

3.88 However, Ms King-Siem went on to argue that:

> It is very hard for us to argue greater protection if we do not offer it within our own jurisdiction.[100]

3.89 Ms King-Siem suggested:

98 Australian Association of National Advertisers and others, *Australian Best Practice Guide for Online Behavioural Advertising*, March 2011.

99 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 22.

100 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 22.

> A starting point would be, and Australia is a signatory to, the [International Covenant on Civil and Political Rights], yet we have not actually brought in our own protections to an adequate level.[101]

3.90 Google discussed the issue from its perspective of a major web-based organisation operating in multiple jurisdictions around the world:

> How does a provider that operates in many different countries, and that in our case seeks to provide a consistent global product with a consistent policy and a set of terms and conditions underpinning that product, meet differing legal requirements? I guess ultimately it is a matter for legal analysis as to which particular laws we have to comply with. We are bound by the laws in countries that we operate...I think it is fair to say that in some respects European privacy law is amongst the most prominent legal models in the world and something that all providers need to take account of.[102]

3.91 The Privacy Commissioner, Mr Pilgrim, explained the issues faced by his office with respect to transborder data flows:

> Regulating privacy online can be difficult due to the greater ease with which personal information can flow between jurisdictions. Like other regulatory schemes, domestic privacy laws may struggle to cope with the ubiquitous nature of the internet. In Australia, organisations that send personal information overseas for processing continue to have obligations under the Privacy Act with regard to that information. The Privacy Act also contains provisions to allow extraterritorial operation where an overseas organisation carries on a business in Australia and collects or holds that information in Australia, and the current reform process is working to enhance those provisions.[103]

3.92 The Privacy Act does not apply to organisations not incorporated in Australia, unless:

- an act or practice of the organisation relates to the personal information of an Australian citizen or permanent resident; and
- the organisation carries on business in Australia and collects or holds the information in Australia.[104]

3.93 The OPC submitted that there is uncertainty as to how this provision operates with respect to personal information submitted over the internet by an individual in Australia to an organisation based overseas:

---

101 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 15.

102 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 6.

103 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 17.

104 *Privacy Act 1988*, s. 5B.

> Given that the internet has allowed greater transfer of personal information across national boundaries, clarifying the scope of extra-territorial operation of the Privacy Act would enhance the Office's ability to apply the Act in these circumstances.[105]

3.94 The OPC has suggested that the requirement for information to have been collected *in* Australia is ambiguous, because in a situation where an Australian submits information to an organisation based overseas, it is unclear whether the overseas organisation has collected information at the point of upload (Australia), or wherever the recipient organisation is based. The OPC has recommended amending the Act to specify that information collected *from* or held in Australia is subject to the privacy principles.[106]

3.95 The exposure draft of amendments to the Privacy Act intends to clarify this issue.[107] However the OPC has submitted to the Senate Finance and Public Administration Committee that the proposed amendments do not resolve the existing uncertainty of the provision. OPC submitted that 'the exposure draft's changes to [section] 5B…do not clarify the issue of where online collection occurs'.[108]

Recommendation 5

3.96 The committee recommends that item 19(3)(g)(ii) of the exposure draft of amendments to the *Privacy Act 1988* be amended to provide that an organisation has an Australian link if it collects information *from* Australia, thereby ensuring that information collected from Australia in the online context is protected by the *Privacy Act 1988*.

3.97 The committee notes that there may be some enforcement challenges relating to this provision, but does not consider that this reduces the need for this reform to proceed.

3.98 The OPC's submission indicates that the issues associated with the transnational nature of online transactions are likely to increase the risk to privacy as 'cloud computing' becomes more ubiquitous. Cloud computing involves the outsourcing of data processing and storage to organisations based overseas. The OPC submitted that:

> While cloud computing may offer benefits to Australian organisations and agencies, the Office considers that there may be some privacy risks associated with use of cloud computing that should be addressed to ensure compliance with Australian privacy laws.[109]

---

105 OPC, *Submission 16*, p. 14.

106 OPC, *Submission to Senate Finance and Public Administration Legislation Committee Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation*, June 2010, p. 44.

107 Item 19(3)(g).

108 OPC, *Submission to Senate Finance and Public Administration Legislation Committee Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation*, June 2010, p. 44.

109 OPC, *Submission 16*, p. 31.

3.99 In this regard the committee received information from Macquarie Telecom which sounds a timely warning on the reduced protections accruing to personal data hosted in the US by a US 'cloud provider':

> It would be extremely difficult to enforce a statutory right arising under Australian law in the U.S., as those laws would not necessarily have extraterritorial effect. Even if a contract with a U.S. Cloud provider is governed by Australian law (which is unlikely under standard terms), enforcement of that contract in a U.S. Court will require expert evidence as to the interpretation and effect of the Australian law, which is costly and difficult.
>
> A U.S.-based Cloud provider would be required to comply with U.S. laws and obey all orders issued by a U.S. Court, even if compliance caused the provider to violate an order issued by an Australian Court.
>
> Even where there is no conflict between U.S. and Australian law, a U.S. court is not obligated to automatically give effect to the orders of an Australian court... [F]or a U.S. court to give effect to an Australian judgment...it would have to be shown that the U.S.-based Cloud provider was subject to Australian law and had been given adequate notice and an opportunity to be heard by the Australian court, and that the Australian order did not offend the public policy of the U.S. forum state.[110]

3.100 NPP 9 and proposed APP 8 require that Australian organisations which send personal information overseas ensure that the data held overseas is governed by privacy laws substantially similar to the Privacy Act, or that contracts prevent overseas affiliates from releasing or using the information other than in accordance with the Privacy Act. In addition, APP 8 will require agencies and organisations to notify individuals if they are likely to disclose personal information to overseas recipients. The OPC supports this change, and recommends that organisations which use cloud computing conduct privacy impact assessments.[111]

3.101 However, Professor Graham Greenleaf and Mr Nigel Waters submitted to the Senate Finance and Public Administration Committee that proposed APP 8 does not address many problems with cross-border data transfers. For example, they argue that:

- individuals are not required to be given notice of any breaches by an overseas recipient and so have no way of proving a breach;
- there are no requirements that individuals be notified of the fact that their personal information is to be sent overseas prior to, or at the time that it is sent; and

110 Macquarie Telecom, *Submission 28, Attachment 1: The Cloud and US-Cross Border Risks*, Freshfields Bruckhaus Deringer, pp 6–7.

111 OPC, *Submission 16*, pp 32-33.

- there are numerous ways in which an exporter of data can be exempt from being accountable for the security of personal information sent overseas.[112]

3.102 The committee notes that the above discussion of the small business exemption provides a mechanism by which an exporter of data can be exempt from accountability for personal data sent overseas. The small business exemption means that over 90 per cent of Australian companies may freely send personal information to overseas companies without ensuring that the privacy of those to whom the information relates will be protected.[113]

3.103 Professor Greenleaf and Mr Waters recommend that APP 8 be amended to provide that rather than an Australian organisation being able to transfer personal information overseas if it *reasonably believes* that the information will be protected in a similar manner to under the Privacy Act, the information must *in fact* be protected in a manner similar to under Australian law.[114] This suggestion would bring Australian law more into line with European privacy regulation under which personal data may only be transferred to a non-EU country if that country can provide adequate protection or if the data controller can personally guarantee that the data will be protected.[115]

3.104 Under Article 29 of the EU Data Protection Directive, a working party was created to advise on the level of protection in non-EU countries. The working party has negotiated data protection agreements with various non-EU countries, including the 'Safe Harbor Principles' between the EU and the United States of America.

3.105 While the Safe Harbor Principles have attracted a degree of criticism, including during this inquiry,[116] they doubtless provide a greater degree of certainty with respect to the protection of personal information transferred offshore than does a requirement that the organisation transferring the data have a 'reasonable belief' that the data will be protected.

---

112 Professor Greenleaf and Mr Waters, Senate Finance and Public Administration Legislation Committee, Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation, *Submission 25*, pp 13–15, at www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/submissions.htm (accessed 23 September 2010).

113 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

114 Professor Greenleaf and Mr Waters, Senate Finance and Public Administration Legislation Committee, Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation, *Submission 25*, p. 14.

115 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed 7 January 2011).

116 See Dr Roger Clarke, Chair, Australian Privacy Foundation, *Committee Hansard*, 1 December 2010, p. 10; Ms Georgia King-Siem, Vice President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 20.

Committee comment

3.106 The committee supports the suggestion of Professor Greenleaf and Mr Waters with respect to the strengthening of Australia's offshore data transfer provisions under the Privacy Act. The committee urges that the exposure draft of amendments to the Privacy Act be amended to take account of this suggestion, and ensure that Australian organisations are fully accountable for protecting the privacy of the personal information they send overseas.

3.107 Furthermore, the committee considers that, while the small business exemption ought to remain in the *Privacy Act 1988*, the provisions relating to the offshore transfer of personal information must apply to all Australian organisations.

3.108 Accordingly, the committee recommends that the government strengthen Australia's privacy legislation to require all Australian companies which transfer personal information offshore are accountable for protecting the privacy of that data. The committee further recommends that the government consider ways to strengthen and ensure the enforceability of such provisions.

Recommendation 6

3.109 The committee recommends that the government amend the *Privacy Act 1988* to require all Australian organisations that transfer personal information offshore are fully accountable for protecting the privacy of that information.

3.110 The committee further recommends that the government consider the enforceability of these provisions and, if necessary, strengthen the powers of the Australian Privacy Commissioner to enforce offshore data transfer provisions.

3.111 The committee notes that the government will consider the powers and functions of the Privacy Commissioner as part of its response to ARLC report 108.

3.112 However, even if Professor Greenleaf's and Mr Waters' recommendation is implemented, the capacity of Australian legislation to protect the privacy of Australians online will remain limited and will depend on the cooperation of overseas organisations and law enforcement agencies.[117] For this reason, the OPC and Victorian Privacy Commissioner have argued that legislation alone is not sufficient to protect the privacy of Australians online.

3.113 In this regard, the Privacy Commissioner, Mr Pilgrim, informed the committee that:

> To further enhance the ability of the privacy regulators to protect personal information, there has been considerable work done to strengthen international cooperation on privacy regulation. This has included development by APEC of cross-border privacy enforcement arrangements to facilitate the handling of privacy complaints between jurisdictions. As

117 Victorian Privacy Commissioner, *Submission 13*, pp 8–9.

> well, there is continuing activity through the OECD's working party on privacy and internet security issues.[118]

3.114 However, the committee notes the concerns expressed by the Australian Privacy Foundation (APF) about the weakness of the APEC Privacy Framework. Dr Clarke, Chair, APF, argued that:

> The US has actually tried to ratchet the standards down even further than their current five eighths by coming up with an APEC Privacy Framework. They endeavoured to use the very low regard that privacy is held in in East Asian cultures as a means of coming up with an alternative privacy framework and sets of principles which would be even weaker than their own FTC administered scheme.[119]

3.115 Ms King-Siem, Vice President, Liberty Victoria, expressed similar concerns, stating that:

> There was certainly an impression that APEC was being used as a bit of a cat's paw for the same purpose [of weakening the safe harbor principles].[120]

Recommendation 7

3.116 The committee recommends that the Australian government continue to work internationally, and particularly within our region, to develop strong privacy protections for Australians in the online context.

Statutory cause of action for breach of privacy

3.117 In addition to working internationally, a number of witnesses pointed out that there is more the government could do to protect Australian's online privacy. Several submitters argued for a statutory cause of action for invasions of online privacy.

3.118 For example, Ms King-Siem, Vice President, Liberty Victoria, argued that a key way in which the Australian Government could strengthen privacy in Australia would be to enact a statutory right to privacy:

> ...government has a real role to play and should be supporting, rather than taking a prescriptive attitude to what information is out there. A general right to privacy, for instance, would put the power back into the hands of Australians. In a lot of cases they probably would not have the wherewithal to take action directly, but at least it puts it back in their hands and it means that they can enforce their rights against whoever is infringing them, be that a corporation, another individual or any other sort of person. At the moment our legislative regime does not really provide for that at all.[121]

---

118 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 17.

119 Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 10.

120 Ms Georgia King-Siem, Vice President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 20.

121 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, pp 15–16.

3.119 Ms King-Siem continued:

> I would have thought that the role of government is to support where possible the users' right to privacy. The fact that we do not actually recognise the right to privacy is slightly problematic in that regard. That would probably be the first argument I would put if we had an independent right to privacy, which the Australian courts have said for a long time that we should have but have been unwilling to step forward and recognise that in a meaningful way because they have been sitting back waiting for the legislature to do it, which so far has been rather unwilling. If that were the case then you would probably see an awful lot of class actions jumping up here and there and that would bring corporations into line a lot faster. That is where you are really letting market forces determine where privacy would lie.[122]

3.120 The ALRC has also recommended the development of a statutory cause of action for serious invasions of privacy.[123] The ALRC considered both statutory and common law causes of action for breach of privacy in other, comparable jurisdictions including the United States, Canada, Ireland, the United Kingdom, the EU and New Zealand and concluded that the development of a statutory cause of action would allow the Australian government to take a more flexible approach to defences and remedies, and avoid some of the issues experienced in other jurisdictions which only have common law causes of action.[124]

3.121 The Victorian Privacy Commissioner, APF and Law Institute of Victoria all indicated support for this recommendation of the ALRC in their submissions to this inquiry.[125] The government has not yet responded to this recommendation, but has stated that it intends to do so in the second stage of its response to the ALRC's report.[126]

Recommendation 8

3.122 The committee recommends that the government accept the ALRC's recommendation to legislate a cause of action for serious invasion of privacy.

---

122 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 20.

123 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, recommendations 74-1–74-5.

124 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, paras 74.112–74.118.

125 Victorian Privacy Commissioner, *Submission 13*, pp 3–4; APF, *Submission 14*, p. 2; LIV, answer to question on notice, 1 December 2010, p. 3. The LIV's support is qualified in a number of respects which are specified in its answer.

126 Senator the Hon Joe Ludwig, Cabinet Secretary, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108*, October 2009, p. 14.

Chapter 4

Law enforcement challenges arising from online technological advancements

4.1 While new technology has created numerous privacy protection issues for individuals and regulators in the online environment (as discussed in chapter 3), developments in web-based technology have also made it possible for individuals and organisations to obscure their identities in a range of circumstances. This has created a number of challenges for law enforcement, and led to a recent controversial proposal from the Attorney-General's Department to require internet service providers to retain specified personal data for law enforcement purposes.

A data retention proposal

4.2 A number of submitters commented on reports and rumours that the Commonwealth Attorney-General's Department was considering implementing a mandatory data retention framework.[1] Prior to this inquiry, very little was known about the proposal, and submissions relied on information from scant news reports.

4.3 On 16 June 2010, an article was published on *ZDNet*, a website dedicated to technology news and discussion, reporting that the government was considering implementing a mandatory data retention regime similar to that in place in the EU.[2] The *ZDNet* report explained that:

> Data retention requires telecommunications providers, including internet service providers (ISPs), to log and retain certain information on subscribers for local enforcement agencies to access when they require it.
>
> The regime sees certain data logged before any suspect is identified, meaning that every internet users' online activities are logged by default.[3]

4.4 The report also noted that various ISP sources have claimed that the mandatory data retention regime 'could extend as far as each individual web page an internet user had visited', however the Attorney-General has denied that web browser history would be logged.[4]

4.5 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, reiterated this point when she appeared before the committee, also explaining that the government is only

---

1 See for example Pirate Party, *Submission 4*, p. 6; Rule of Law Institute of Australia, *Submission 17*.

2 Ben Grubb, 'Inside Australia's data retention proposal', ZDNet, 16 June 2010 at www.zdnet.com.au/inside-australia-s-data-retention-proposal-339303862.htm (accessed 15 September 2010).

3 Ben Grubb, 'Inside Australia's data retention proposal', ZDNet, 16 June 2010.

4 Ben Grubb, 'Inside Australia's data retention proposal', ZDNet, 16 June 2010.

considering the retention of 'metadata' in relation to online communications, and not content.[5]

4.6 Ms Smith also emphasised that no decision has been made by government yet about whether to implement such a regime:

> I should say that no decision has been made by government about a data retention proposal.[6]

4.7 However, even at this early stage, there was a lot of confusion amongst witnesses about the specifics of the proposal and particularly about what information would and would not be retained. It seems that this is due to the limited range of organisations with which the Attorney-General's Department has consulted on the proposal at this stage.

4.8 A number of witnesses expressed concern about the lack of consultation during the development of the data retention proposal. For example, the Law Institute of Victoria (LIV) criticised the lack of consultation and transparency in the development of the policy to date.[7] Similarly, Dr Clarke, Chair, Australian Privacy Foundation (APF), informed the committee that the APF had been 'unable to get a place at the table in discussions on this matter'.[8] Dr Clarke continued:

> The government will not consult with us. They will consult with industry; they will not consult with civil society. When I say ‘us’, there is no reason why the APF has to be chosen as one of the organisations that government agencies interact with if there are other alternative organisations that cross into the same space. Civil liberties organisations do; in other contexts, consumer organisations do. Our argument is that civil society is not being engaged...[9]

4.9 Officers from the Attorney-General's Department disputed this, informing the committee that:

> We actually did consult with a broad range of people and have done so over some time within the industry.[10]

4.10 Ms Smith specified that the Department had consulted with the following organisations:

- ISPs;

---

5 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 53.

6 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

7 Law Institute of Victoria (LIV), *Submission 9*, p. 1.

8 Mr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 9.

9 Mr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 9.

10 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 88.

- 'a wide range of the carrier network';
- bodies like the Internet Industry Association, the Communications Alliance and the AMTA [Australian Mobile Telecommunications Association];
- state and Commonwealth agencies including non-interception agencies like ASIC and ACCC; and
- the Office of the Privacy Commissioner.[11]

4.11 Ms Smith concluded that:

> It was very broad consultation within government and industry.[12]

4.12 Ms Smith explained that the purposes of consultations on the data retention proposal to date were 'for the purposes of developing a model, not to actually consult on a model'.[13] She argued that the proposal is not yet at a stage where it was appropriate to begin consultations with public interest and privacy advocacy organisations:

> In regard to the development of this particular issue, to date we are still not at a point where we think it is suitable to actually go out for that further consultation. In any policy development, you have to look at the outcome you are trying to achieve, the problem and how to address the problem, and you have to talk to the key stakeholders to see what is viable. When I say key stakeholders, I am talking about the agencies and the industry that are going to be primarily working to effectively build a solution. We do not want to pre-empt consultation with the public until we have a view around what that could possibly be.[14]

The EU mandatory data retention scheme

4.13 A model of mandatory data retention has existed in the European Union since March 2006. EU Directive 2006/24/EC requires Member States to adopt measures to ensure that metadata related to email, telephony and internet access is retained for between six months and two years.[15]

---

11 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 88.

12 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 88.

13 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 89.

14 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 48.

15 Directive 2006/24/EC of the European Parliament and of the Council, 15 March 2006, Official Journal L105, 13/04/2006, pp 54-63, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML, (accessed 18 October 2010).

4.14 Metadata is the information about the communication—the time and location—proving the fact that it occurred, rather than information about its content.[16] The EU Directive specifies that member states must require the retention of the following metadata:

- data necessary to identify the source of a communication (e.g. the name and address of the subscriber, phone number, user identification etc);
- data necessary to identify the destination of a communication (e.g. the phone number or email address of the recipient and their name and address if they subscribe to the same service/network);
- data necessary to identify the date, time and duration of a communication (including the time a user logs in and out of their internet access service);
- data necessary to identify the type of the communication;
- data necessary to identify users' communication equipment (e.g. the digital subscriber line (DSL) or telephone number);
- data necessary to identify the location of mobile communication.[17]

4.15 Article 5(2) provides that 'no data revealing the content of the communication may be retained pursuant to this directive'.

4.16 The EU Directive is still in the process of being implemented into national law, however in some countries where it has already been implemented, the laws have attracted significant controversy. For example, EFA noted:

> In March this year [2010], Germany's Federal Constitutional Court suspended German law implementing the Directive, ruling it was unconstitutional. Among other reasons, they cited a lack of transparency in the potential uses of the data.[18]

4.17 Mr Jacobs, Chair, EFA, informed the committee that in that case:

> The judge pointed out that even though it was just the data about communications there would be sufficient data gathered to enable the compilation of a profile on somebody's interests, which political party they might be leaning towards, et cetera, and that it was out of proportion to the needs of law enforcement.[19]

4.18 There has also been criticism of the Directive by other EU members and by prominent civil liberties organisations. For example, Mr Jacobs explained:

---

16 Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 96.

17 Directive 2006/24/EC of the European Parliament and of the Council, 15 March 2006, Official Journal L105, 13/04/2006, pp 54–63, Article 5.

18 EFA, *Submission 20*, p. 2 (references omitted).

19 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 62.

> Sweden has declined to implement the directive and so they are subject of a suit by the European Commission. In Romania a court found that the data retention provisions violated the European Convention on Human Rights. Also the ACLU [American Civil Liberties Union] and others have come out and claimed that data retention schemes such as this one are in violation of the Universal Declaration of Human Rights, and I believe that others have pointed out in their submissions to the committee that you would violate the National Privacy Principles in Australia including fairness, being unobtrusive, and collecting data only for its stated purpose.[20]

4.19 When asked about the impact of the EU directive on Google's global operations, Mr Flynn, Head of Public Policy and Government Affairs, Google Australia said:

> Our view is that any requirement to retain data to enable the investigation and detection and prosecution of serious crimes has to be proportionate to the resultant privacy impact and anonymity loss for internet users, as well as the costs to search providers of implementing something like that. I guess the key thing that we would take out of it is transparency. That is something that we emphasise in our efforts around privacy and we think it is very, very important.[21]

4.20 Mr Flynn continued:

> On the transparency front, we have launched a tool which you may have seen. It is a website and it actually gives details of the requests we get from governments around the world for two things. One is for data on users and the second is requests to remove content from our different services—like YouTube, for example. We think it is important because it is a step on the road to having greater transparency around these kinds of efforts and we think that is important. We would be interested to see others in industry take the same kind of approach.[22]

Current practice in Australia

4.21 Currently in Australia the data retained about an individual's online communication and internet usage may be used for law enforcement purposes in certain circumstances.

4.22 Australian Internet Service Providers (ISPs) are required to comply with the *Privacy Act 1988* with respect to personal information of their customers. However, they are also required to:

- assist authorities in enforcing the law;

---

20 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 62.

21 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 5.

22 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 5.

- do their best to prevent their network from being used to commit offences; and
- ensure that authorities are able to intercept communications through their network in accordance with a validly issued warrant or order.[23]

4.23 Under Part 4-1 of the *Telecommunications (Interception and Access) Act 1979* the head, deputy head or authorised officer of a law enforcement agency may authorise the disclosure of documents or information if satisfied that the disclosure is reasonably necessary for the enforcement of criminal law, to impose a pecuniary penalty, or to protect public revenue.[24] The content or substance of communications (e.g. the contents of an email) cannot be obtained through this method, only the metadata.[25]

4.24 Authorisation may also be given for information likely to be collected in the future if the authorised officer is satisfied that such disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years.[26]

4.25 In order to obtain the content of online communications, law enforcement must obtain a warrant.[27]

4.26 Ms Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, advised the committee that while law enforcement agencies currently have the legal power to access the metadata from online communications, through the above described method, they can only do so if the relevant online service provider has retained the metadata, which there is currently no requirement for them to do.[28]

4.27 Ms Smith explained:

> The development of a data retention proposal is intended to ensure a national and systematic approach is taken for the availability of telecommunications data for investigative purposes. Data retention would not give agencies new powers. It would ensure that existing investigative capabilities remained available.[29]

---

23 ACMA, 'Internet Service Providers and Law Enforcement and National Security Fact Sheet', at www.acma.gov.au/WEB/STANDARD/pc=PC_100072 (accessed 28 September 2010).

24 *Telecommunications (Interception and Access) Act 1979*, ss 178 and 179.

25 *Telecommunications (Interception and Access) Act 1979*, s. 172.

26 *Telecommunications (Interception and Access) Act 1979*, s. 180.

27 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

28 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

29 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

4.28 Ms Smith informed the committee that 'telecommunications data is an important investigative tool' which provides 'important leads for agencies, including evidence of connections and relationships'.[30] Law enforcement agencies have come to rely on the information kept by traditional methods of communication, such as fixed-line phones. Ms Smith explained:

> In the good old days when we all had a fixed-line phone there was information kept about—for example, I called someone, their phone number, for how long, how much it cost, all that sort of information.[31]

4.29 Data about that telephone call, which was collected by the telephone company for billing purposes, could then be used by law enforcement agencies following the procedure under the *Telecommunications (Interception and Access) Act 1979* for investigations, and to provide evidence justifying a warrant, for example for a telephone interception.

4.30 However, more modern forms of communication, such as Voice over Internet Protocol (VoIP), and email do not require providers to retain detailed information for billing purposes. Ms Smith told the committee:

> Internet based service providers tend to charge on the quantity of data used rather than on a per call basis. Over time, as telecommunications services such as voice-telephone migrate to voice-over-internet based services, less and less information will be retained and stored. Therefore, this means that traditionally available telecommunications data—as: 'Person X called person Y at this time'—may no longer be available.[32]

4.31 This means that the information is less likely to be retained by providers, and therefore, even though law enforcement may have the power to obtain it, it does not exist. Ms Smith explained:

> Despite the increased reliance on telecommunications data and the acknowledgement of the importance of telecommunications data, industry have confirmed that there will be changes to and reductions in the type of telecommunications data which will be retained into the future. They indicate that this is a natural evolution as a result of advances in technology and business models. For example, the telecommunications sector is quickly migrating from the traditional telephone network to internet protocol based networks.[33]

---

30 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

31 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 98.

32 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

33 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

The government's proposal

4.32 The Department's proposal for a mandatory data retention scheme is 'intended to ensure a national and systematic approach is taken for the availability of telecommunications data for investigative purposes'.[34]

4.33 At this early stage, it is proposed that metadata 'about the process of communication, as distinct from its content' is retained by telecommunications and internet service providers.[35] Ms Smith, likened this metadata to the information retained by fixed-line phone companies for billing purposes—information about who contacted whom and when.[36]

4.34 Ms Smith emphasised to the committee that no decision has yet been made by government about a data retention proposal.[37] However, the Department has developed a 'data set' of the categories of information to be retained and has also engaged in discussions with industry about the data set and the period for which data would be retained.[38]

4.35 Those consultations revealed that:

> Advice from industry is that the majority of information that is included in that draft data set is currently retained. The issue is the length of time it is retained for. Some of the information is retained for days whilst some of it is retained for years. Some of that information is retained for audit and taxation purposes. Each individual industry participant currently holds a vast amount of information on every one of their customers.[39]

4.36 The Australian Federal Police (AFP) argued that a mandatory data retention scheme would not give the police additional powers, and that 'all we are asking for here is for the status quo to remain'.[40]

---

34 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

35 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

36 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 98.

37 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

38 Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, pp 87–88. The Department provided the committee with a copy of the data set on a confidential basis.

39 Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 50.

40 Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations, AFP, *Committee Hansard*, 29 October 2010, p. 87.

4.37 Assistant Commissioner Gaughan gave an example of when communications metadata has proven useful for law enforcement purposes, of Operation Centurion, a child pornography investigation:

> Centurion was a 2008 investigation in which the AFP received a number of referrals in relation to a particular activity. All we received to commence our investigation with were a number of Australian IP, internet protocol, addresses. As a result of that investigation we were able to go back to the metadata and ascertain that there were a large number of Australians who were involved in possessing child abuse material, because the ISPs had retained that information, which enabled us to then take actions in progress. As a result of that we executed in excess of 340 search warrants, we arrested in excess of 140 people, we seized 400,000 images and, more importantly from my perspective, we actually saved four children who were potentially at risk from child abuse. Without that metadata being retained, the AFP cannot do those types of investigations because we will not have that information to backtrack.[41]

4.38 In a private session, the committee heard details of a range of other ongoing investigations, which the Department and the AFP argued demonstrated why telecommunications data is an important investigative tool.[42]

Criticisms of the data retention proposal

4.39 The Attorney-General's Department's proposed data retention scheme attracted a great deal of criticism from witnesses and submitters. Major arguments against the proposal included that it:

- is inconsistent with the Privacy Act and its principles, and an unnecessary invasion of privacy generally;
- treats online and offline information differently without reason; and
- that it is unlikely to be effective or useful to law enforcement.

Breach of privacy principles

4.40 The Law Institute of Victoria (LIV) submitted that the proposal is inconsistent with the National Privacy Principles, as the information collected is unnecessary for both the functions of the ISP and in the vast majority of instances for law enforcement agencies.[43]

4.41 Specifically, the LIV identified that the proposal contradicts NPP 4.2 which relates to the time period that information is retained. NPP 4.2, which is included in proposed APP 11 in the government's Exposure Draft of amendments to the Privacy Act, provides that any personal data which is held by an organisation and is no longer

---

41 Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations, AFP, *Committee Hansard*, 29 October 2010, p. 89.

42 The committee conducted *in camera* hearing with officers from the Attorney-General's Department and the Australian Federal Police on 1 December 2010.

43 LIV, *Submission 9*, p. 1.

required for the purposes for which it was obtained, should be destroyed or de-identified. Ms Miller, Law Institute of Victoria, argued:

> Our opinion of that principle when applied to this policy is that this information could potentially be retained indefinitely because, basically, how is an ISP to know when a law enforcement agency no longer needs the information that is being collected for them?[44]

4.42 Ms Miller explained that requiring ISPs to retain enormous quantities of data for an extended period also leads to concerns about data security:

> There is also a concern about the sheer magnitude of the information that needs to be collected. That would all need to be stored somewhere, and the ISPs would have obligations under the National Privacy Principles to protect against the misuse of that data. The sheer scale of the information collected raises questions about how that would happen.[45]

4.43 The Privacy Commissioner, Mr Pilgrim, agreed that this was a concern:

> One of the issues that we face when we are looking at the retention and collection of personal information are the risks that are going to be associated with holding information for a long time when there may not be necessarily a clear or defined purpose for it. If you hold information—whether it be in databases or even if we look at it in the old style of a filing cabinet—and have it sitting around for a long time there is often a great risk that something could happen to it. It could be mishandled or used for inappropriate purposes.[46]

4.44 The LIV also raised concerns about the inconsistency of a data retention scheme with NPPs 8 and 10 (which are included in proposed APPs 2 and 3 respectively). Ms Miller argued that:

> The problem with the amount of information that is being collected about people is that it renders it almost impossible to be anonymous, because of the profile that can be developed about you. Also, some of the information may include 'sensitive information', as defined under the principles, which is things such as gender, political opinion, sexual preferences and health information.[47]

---

44 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

45 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24. The LIV submission made similar points by referring to the risks of data misuse, loss, and unauthorised access associated with requiring ISPs to retain such vast quantities of data; *Submission 9*, p. 2.

46 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 18.

47 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

4.45 Mr Jacobs, Chair, Electronic Frontiers Australia, noted that even though the government is not proposing to require ISPs to retain the content of online communications 'it is still very, very possible to use information of the kind that you described—when an email was sent and to whom—to build up a profile of somebody's habits'.[48] Mr Jacobs argued that this level of monitoring is unnecessary and invasive:

> Even if you do not know the content of the webpage that somebody viewed or the information that they posted in a form when they interacted with the website, just knowing what websites they go to and the fact that they are using them would enable you to build up a full profile of somebody's interests and habits.[49]

4.46 Mr Jacobs argued that the proposal has significant privacy implications, describing it as 'mass surveillance':

> The scheme as proposed has huge drawbacks as well for a society, and we have yet to hear a very good case for why such power should be necessary. We do not think it is hyperbolic to describe such a system has 'mass surveillance' because it does involve the most private communications of pretty much everybody in the country who uses the internet for communication—and if it is not everybody yet, it is going to be.[50]

4.47 Furthermore, Mr Jacobs argued that there was no justification for the proposal:

> I have not heard a compelling case that the system we have now is broken. With a warrant, with a court order, a law enforcement agency can go to a company that provides email services, like Google or Yahoo, or to an internet service provider and determine the identity of somebody who was at a particular IP address or view their emails. Until I hear a compelling case that that is just not enough data, that we need to go further back in time, that we need to have the information on everybody, whether or not they are of interest to law enforcement at the moment, we certainly cannot support the data retention proposal.[51]

4.48 The Privacy Commissioner, Mr Pilgrim, agreed with the general principles espoused by EFA, Liberty Victoria and the LIV, and was uncomplimentary about the proposal generally (although he did not comment on its specifics). Mr Pilgrim stated:

> A central principle in the Privacy Act is that agencies and organisations should only collect the personal information that is necessary for their functions or activities. Generally, my office would not support the collection of personal information on the chance that it may be just useful at some later date. As noted in our submission: … broad scale collection and

48 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 68.

49 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 69.

50 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 61.

51 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, pp 71–72.

> retention of web browsing information could significantly impact on the privacy of individuals.[52]

4.49 Mr Pilgrim explained that it is important to ensure that for any data retention proposal:

> …we need to first of all understand what the exact problem is that is trying to be responded to by proposing something such as data retention. Is the response—be it setting a timeframe of six months, one year, two years or however many years—proportionate to the risk that is being proposed? You need to clearly understand what the risk is that we are trying to address by maintaining and keeping this information.[53]

4.50 Mr Pilgrim suggested that before any proposal is implemented a privacy impact assessment should be done to identify the risks to privacy, including requiring ISPs to hold personal data for an extended period of time.[54]

4.51 Mr Pilgrim also noted that:

> One of the other key issues that we would need to see addressed in any proposal for data retention is what the accountability mechanisms are going to be. Are there sufficient accountability mechanisms to ensure that if that information is being held it is being held securely and that it is not being misused or used for any other purpose that would be beyond the expectation of the individual? Finally, there should be review mechanisms to ensure that those processes are in place and to make sure that, for example, the risk that led to the establishment of those sorts of proposals is still there and still warrants that sort of retention.[55]

4.52 The importance of accountability and appropriate oversight was also emphasised by the Rule of Law Institute and Electronic Frontiers Australia.[56]

The proposal treats online and offline information differently

4.53 A second key concern of submitters and witnesses opposed to the data retention proposal was that it treats online and offline information differently. Ms Miller of the Law Institute of Victoria, noted:

> The best way of illustrating that is simply to point out that if this proposal was that all mail sent and received within Australia be logged and retained for seven years, or that all phones be intercepted and recorded, then I think

---

52 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, pp 17–18.

53 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

54 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

55 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

56 Rule of Law Institute of Australia, *Submission 17*, p. 2; Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 72.

> it is not stepping outside the bounds of my expertise to say that there would be significant public outcry. What we have here is the electronic equivalent, and it really means that the government is proposing to treat online privacy in a way that is different to offline privacy simply because the technology makes it possible.[57]

4.54 Ms Miller argued that there is no justification for treating online and offline privacy differently:

> I do not think that people make that distinction in their personal lives, their private lives, their professional lives. We do not think that it is appropriate that the parliament make a distinction in legislation between online privacy and offline privacy.[58]

4.55 Ms Miller surmised that when it comes to the possible benefits of technology, law enforcement agencies seem to ask 'Can we do it?' as opposed to 'Is it appropriate or reasonable to do it?', and use invasive investigative techniques because they can, rather than because it is appropriate.[59] She argued:

> The question should always be 'Is it appropriate and reasonable?' It should not be the case that just because we can we will.[60]

4.56 Mr Pilgrim, Privacy Commissioner, agreed that it is not appropriate to distinguish between online and offline privacy simply because it is possible:

> I would say that my position is that I would favour a consistent approach to data protection. I have not seen demonstrated necessarily why there should be any difference between whether the information is being handled online or offline. I have not seen a strong case put forward to explain that to me. [61]

4.57 In response to arguments by the Attorney-General's Department and the AFP that the proposal simply retains the status quo, requiring the retention of the same information that is available in relation to fixed-line telephone calls to be retained for

---

57 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

58 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 25.

59 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 25.

60 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 25.

61 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 18.

online communications,[62] many witnesses strongly disagreed. For example, Ms Miller argued:

> The first distinction that I would make between call charge records and metadata of internet websites is that a phone number is just a phone number unless you have other information to interpret what the phone number is. And even if you know who owns the phone number and who the usual users of that number might be, you still know very little about the content of the conversation. I would suggest that when it comes to websites the website address and the type of information that is commonly found on that website can in fact be readily ascertained, even just from the metadata. So, even if the proposal is restricted to metadata as opposed to the actual web pages, there is still a great deal of extra information that can be obtained that you could not get from something like a call charge record.[63]

4.58 Another difference that Ms Miller noted was the important fact that data relating to fixed line telephone calls is collected for billing purposes, not law enforcement purposes. ISPs do not need to retain metadata for billing purposes, so that 'the only reason that they would be collecting this information is because it might be useful to law enforcement agencies not because of how they provide or charge for their service'.[64]

4.59 The LIV argued that this is inconsistent with key recommendations in the ALRC's report on Australian privacy law and practice,[65] submitting that:

> The large-scale collection of personal information by governments because it *may* be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet.[66]

4.60 Ms King-Siem, Vice President, Liberty Victoria agreed:

> I understand security issues, but this is where you take a targeted approach where there is a justification and reasonable suspicion that that information is required, not collect information and worry about it later. I think there is a tendency both at government and at corporate level—and in fact it is

---

62 Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations, AFP, *Committee Hansard*, 29 October 2010, p. 87.

63 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 26.

64 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 26.

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

66 LIV, *Submission 9*, p. 2. Emphasis in original.

> perhaps just a natural tendency—to collect more than you need and then swallow it later.[67]

Will the data be useful for law enforcement

4.61 Finally, a number of witnesses and submitters questioned whether the data proposed to be retained would even be of use to law enforcement.

4.62 The LIV argued that the proposed regime would be 'unworkable for law enforcement agencies' due to the huge amounts of data collected.[68]

4.63 Ms Miller, LIV, also argued that the proposal is unnecessary as:

> Law enforcement agencies can currently apply for warrants to obtain information such as browsing histories from ISPs. If there is a concern that some ISPs do not contain significant browsing history, then the LIV considers that that can be dealt with on a case-by-case basis.[69]

4.64 There is also a risk that a data retention scheme will be ineffective because criminals and others wishing to evade detection will simply use the various mechanisms available to them to hide their online identity. The committee received evidence of various international online services dedicated to protecting the identity of domain name owners. For example, Fraudwatch International submitted that:

> Some domain registrars now provide a "Domain Privacy Protection" service, where the domain owners contact information is not listed in the WHOIS database, but is replaced by standard contact information for either the domain registrar or the privacy service, making it virtually impossible to actually find, or contact the real owner of the domain.[70]

4.65 This obviously makes it incredibly difficult to identify the owners of fraudulent phishing websites and shut them down. Mr Trent Youl, CEO, Fraudwatch International, informed the committee that:

> One of the issues we face when we are trying to have phishing websites taken down is that we find a hacked website and suddenly we cannot contact the website owner because their information is hidden. If the website owner has subscribed to this type of service that is apparently protecting their privacy and they do not have any contact information on their website, which many websites do not, it makes it very difficult for us sometimes to do our job and get these fraudulent websites taken down as quickly as possible.[71]

---

67 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 16.

68 LIV, *Submission 9*, p. 2.

69 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

70 Fraudwatch International, *Submission 22*, p. 2.

71 Mr Trent Youl, CEO, Fraudwatch International Pty Ltd, *Committee Hansard*, 29 October 2010, p. 74.

4.66 Fraudwatch submitted that domain privacy protection:

> ...allows people to anonymously run websites which may be using dubious business practices, fraud, or theft [and] it allows criminals to hide their contact information and appear to be legitimate.[72]

4.67 There is a good chance that increased law enforcement monitoring of online communications will result in the proliferation of this, and similar options for internet users to hide their identity, provided that they are sufficiently tech-savvy. Mr Jacobs, Chair, EFA, explained:

> Given that you can host a website in any country and given that regulations vary, the way the internet works is anonymity is something that is probably going to apply to people who run websites as well as people who use them. So I think it is inevitable that such technology will exist. We will see a bit of an arms race when it comes to the technology itself and, perhaps, with the laws; but, no, I do not find that surprising. I think it is inevitable. We will have to have other ways to deal with it.[73]

4.68 There are already services available for consumers who wish to evade the EU's data retention scheme and other monitoring, such as Tor[74] and the Invisible Internet Project (I2P).[75]

Committee comment

4.69 The committee has a number of concerns, both with the Attorney-General's Department's data retention proposal itself, as well as with the way the consultation process has been handled so far.

4.70 There is a lot of misinformation and rumour about the scheme, and it seems to the committee that this is largely due to the Attorney-General's Department's narrow consultations on the issue to date. While industry has been consulted, there has not yet been any discussion with the broader community or public interest and civil liberties organisations. While the committee acknowledges the Attorney-General's Department's explanation for this,[76] the lack of information available to the public about the proposal has resulted in confusion, mistrust and fear about the proposal.

4.71 The committee's central concerns about the proposal are the very real possibilities that it is unnecessary, will not provide sufficient benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved. The proposal has very serious privacy implications, even if one accepts the arguments of the Attorney-General's Department and AFP that the same information is already available for fixed-line telephone records. The fact is that much of the information

---

72 Fraudwatch International, *Submission 22*, p. 4.

73 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 67.

74 www.torproject.org (accessed 12 January 2011).

75 www.i2p2.de (accessed 12 January 2011).

76 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 48.

intended to form part of the scheme does not need to be collected for any other purpose, so the only reason to retain it is the mere possibility that it may prove useful to law enforcement. This seems to the committee to be a significant departure from the core principles underpinning Australia's privacy regulation.

4.72 Furthermore, the committee considers that there is a very real risk that the most serious, tech-savvy criminals—particularly those involved in fraud and child pornography—will be able to evade monitoring in any respect as a result of technological developments.

4.73 Accordingly, the committee urges that prior to any proposal for data retention going any further, an extensive analysis of the costs, benefits and risks of such a scheme must be undertaken. Before pursuing such a scheme, it is incumbent upon government to:

- prove that the information is necessary to law enforcement agencies and justifies such a significant intrusion on the privacy of all Australians;
- quantify and justify the expense to ISPs and other companies which will be required to retain data under such a scheme;
- implement strong and appropriate accountability and monitoring mechanisms, and ensure that data retained under the scheme is able to be, and will in fact be, stored securely; and
- consult with a wide range of stakeholders on the proposal, including, but not limited to, civil liberties and public interest advocates, privacy policy experts such as the Australian Privacy Foundation, in particular.

Recommendation 9

4.74 The committee recommends that before pursuing any mandatory data retention proposal, the government must:

- **undertake an extensive analysis of the costs, benefits and risks of such a scheme;**
- **justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;**
- **quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;**
- **assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and**
- **consult with a range of stakeholders.**

4.75 The committee notes that the government is reviewing cyber security and cyber crime as part of its response to the recommendations of the recent House of Representatives committee report into Cyber crime (see paragraph 1.7).[77] The committee encourages the government to take the recommendations contained in this report into account in that review. The committee also expects the government will respond separately to the recommendations made in this report in the usual manner, noting that the Senate has declared that responses should be tabled within 3 months.[78]

Senator Mary Jo Fisher
Chair

Senator Doug Cameron
Deputy Chair

Senator Scott Ludlam

77 House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, June 2010, www.aph.gov.au/house/committee/coms/cybercrime/report.htm (accessed 7 March 2011); and the government response, 25 November 2010, www.aph.gov.au/house/committee/coms/governmentresponses/cybercrime.pdf (accessed 7 March 2011).

78 Senate Standing Orders, Procedural Order of Continuing Effect no 42, June 2009, p. 140, www.aph.gov.au/Senate/pubs/standing_orders/standingorders.pdf (accessed 6 April 2011).

Appendix 1

Submissions, tabled documents and answers to questions taken on notice

Submissions

1 Mr Arved von Brasch

2 Yahoo!7 Pty Ltd

3 Australian Association of National Advertisers

4 Mr Rodney Serkowski, Pirate Party Australia

5 Confidential

6 Google Australia Pty Ltd

7 Community and Public Sector Union (CPSU)

8 Mr Alastair MacGibbon, Internet Safety Institute

9 Law Institute of Victoria

10 Australian Council of Trade Unions

11 Australian Communications Consumer Action Network (ACCAN)

12 The Communications Council

13 Office of the Victorian Privacy Commissioner

14 Australian Privacy Foundation

15 Australian Direct Marketing Association

16 Office of the Privacy Commissioner

17 Rule of Law Institute of Australia

18 Name Withheld

19 Name Withheld

20 Electronic Frontiers Australia

21 Mr John Scott

22 FraudWatch International Pty Ltd

23 Australian Federation of AIDS Organisations (AFAO)

24 Dr George Barker

25 Business Council of Australia

26 Mr Nigel Waters, Cyberspace Law + Policy Centre, Faculty of Law, UNSW

27 Australian Youth Affairs Coalition

28 Macquarie Telecom

29 iWebgate Pty Ltd

Tabled documents

Distribution list for March 2010 data retention consultation meeting – Communications Alliance (tabled by the Attorney-General's Department, public hearing, Canberra, 29 October 2010).

Opening statement by Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department (public hearing, Canberra, 29 October 2010).

Answers to questions taken on notice

1 Attorney-General's Department - Answers to questions taken on notice (from public hearing 29 October 2010)

2 Australian Association of National Advertisers - Answers to questions taken on notice (from public hearing 29 October 2010)

3 The Communications Council - Answers to questions taken on notice (from public hearing 29 October 2010)

4 Liberty Victoria - Answers to questions taken on notice (from public hearing 1 December 2010)

5 Liberty Victoria - Answers to questions taken on notice (from public hearing 1 December 2010)

6 Australian Council of Trade Unions - Answers to questions taken on notice (from public hearing 1 December 2010)

7 Google - Answers to questions taken on notice (from public hearing 29 October 2010)

8 Australian Direct Marketing Association - Answers to questions taken on notice (from public hearing 29 October 2010)

9 Law Institute Victoria - Answers to questions taken on notice (from public hearing 1 December 2010)

Appendix 2

Public hearings

Friday, 29 October 2010 – Canberra

Google Australia Pty Ltd

Mr Iarla Flynn, Head, Public Policy and Government Affairs

Ms Ishtar Vij, Manager, Public and Policy and Government Affairs

Office of the Privacy Commissioner

Mr Timothy Pilgrim, Australian Privacy Commissioner

Ms Angelene Falk, Director, Policy

Australian Association of National Advertisers

Mr Scott McClellan, Chief Executive Officer

The Communications Council

Mr Daniel Leesong, Chief Executive Officer

Mr Iain McDonald, Board Member

Ms Linde Wolters, Media and Public Affairs

Australian Communications Consumer Action Network

Ms Teresa Corbin, Chief Executive Officer

Australian Direct Marketing Association

Mrs Melina Rohan, Director, Corporate and Regulatory Affairs

Electronic Frontiers Australia

Mr Colin Jacobs, Chair

Fraudwatch International Pty Ltd

Mr Trent B Youl, Chief Executive Officer

Department of Broadband, Communications and the Digital Economy

Mr Keith Besgrove, First Assistant Secretary, Digital Economy Services

Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch

Mr Duncan McIntyre, Assistant Secretary, Consumer Policy and Post

Ms Joan Sheedy, Assistant Secretary, Privacy and Freedom of Information Policy Branch

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Australian Federal Police

Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations

Mr Peter Whowell, Manager, Government Relations

Wednesday, 1 December 2010 – Melbourne

Australian Privacy Foundation

Dr Roger Clarke, Chair

Victorian Council for Civil Liberties (Liberty Victoria)

Ms Georgie King-Siem, Vice-President

Law Institute of Victoria

Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section

Australian Council of Trade Unions

Mr Trevor Clarke, Legal and Industrial Officer

Mr Joel Fetter, Policy and Industrial Director

Australian Federal Police

Commander Alan Scott, Manager, Melbourne Office

Mr Peter Whowell, Manager, Government Relations

Attorney-General's Department

Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Australian Communications and Media Authority

Ms Olya Booyar, General Manager, Content, Consumer and Citizen Division

Ms Nerida O'Loughlin, General Manager, Digital Economy Division

Ms Jonquil Ritter, Executive Manager, Citizen and Community Branch, Content, Consumer and Citizen Division

Ms Andree Wright, Executive Manager, Security Safety and e-Education Branch, Digital Economy Division

Appendix 3

Information Privacy Principles, National Privacy Principles, and proposed Australian 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.

Proposed Australian Privacy Principles

Extract from exposure draft of amendments to the *Privacy Act 1988*, released 24 June 2010.

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

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.