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.