Australian Government

Office of the Privacy Commissioner

The adequacy of protections for the privacy of Australians online

Submission to Senate Standing Committee on Environment, Communications and the Arts

August 2010

Table of contents

Executive Summary

The Office of the Privacy Commissioner (the Office) welcomes the opportunity to provide input to the Senate Standing Committee on Environment, Communications and the Arts (the Committee) inquiry into the adequacy of privacy protections for Australians online.[1]

Since its enactment over twenty years ago, the *Privacy Act 1988* 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. Concurrent with this inquiry is the senate inquiry into the exposure draft of the Australian Privacy Principles (APPs).[2] The APPs, which will replace the existing principles in the Privacy Act, form a significant part of the reform agenda flowing from the Australian Law Reform Commission's (ALRC) review of privacy law and the Government's response to that review.[3]

In this submission, the Office outlines the general coverage of the Privacy Act and reforms recommended by the ALRC that may have a bearing on online privacy. The Office also discusses a number of specific online privacy issues related to: social networking, web 2.0, online behavioural advertising, use of web browsing information for law enforcement, converging technology and ubiquitous computing, and cloud computing.

Key recommendations and observations

The Office makes the following observation:

1. That the best approach to enhancing privacy online will be multi-faceted, comprising:

    i. principle-based legislation (with specific technology issues dealt with under binding codes where desirable and necessary)

    ii. 'end-user' empowerment through education

    iii. privacy enhancing technology design

[1] Terms of reference for the inquiry are available at www.aph.gov.au/senate/committee/eca_ctte/online_privacy/index.htm.

[2] Senate Finance and Public Administration Committee Inquiry into the Exposure Drafts of Australian Privacy Principles, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm.

[3] See Australian Law Reform Commission, *For your information: Australian Privacy Law and Practice*, ALRC 108, 2008, www.austlii.edu.au/au/other/alrc/publications/reports/108/ and Australian Government, *First stage response to ALRC Privacy Report*, 2009 www.dpmc.gov.au/privacy/reforms.cfm.

iv. international cooperation between jurisdictions.

Further the Office makes the following specific recommendations:

2. That the Committee consider as part of its inquiry:

   - the Senate Finance and Public Administration Committee's inquiry into the exposure draft of the APPs in assessing the adequacy of privacy protections for online information handling, and the Office's submission to that inquiry[4]
   - the work of the Australian Parliament Joint Select Committee looking into Cyber-safety[5] and
   - the House of Representatives Standing Committee on Infrastructure, Transport, Regional Development and Local Government inquiry into smart infrastructure.[6]

3. That development and greater use of privacy enhancing technologies (PETs) be promoted with the aim of achieving the following outcomes:

   - ongoing research into, and development of, PETs
   - greater awareness amongst government agencies and private sector organisations as to the existence and desirability of PETs for personal information handling and
   - greater range and availability of PETs (including in off-the-shelf products).

4. That social networking sites be encouraged to:[7]

   - carry out a privacy impact assessment on changes to personal information handling practices[8]

[4] Senate Finance and Public Administration Committee Inquiry into the Exposure Draft of Australian Privacy Principles, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm and Office of the Privacy Commissioner, *Submission to Senate Finance and Public Administration Committee Inquiry into the Exposure Draft of the Australian Privacy Amendment Legislation*, August 2010.

[5] Joint Select Committee on Cyber-safety, *Terms of reference*, www.aph.gov.au/house/committee/jscc/tor.htm.

[6] House of Representatives Standing Committee on Infrastructure, Transport, Regional Development and Local Government, Smart Infrastructure Inquiry, *Terms of reference* www.aph.gov.au/house/committee/itrdlg/smartinfrastructure/tor.htm.

[7] The Office plays a role in helping organisations to avoid acts and practices that may interfere with the privacy of individuals. See for example, *Privacy Act 1988*, s 27(1) (d) and (e).

[8] See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2010, www.privacy.gov.au/materials/types/download/9509/6590.

- be transparent regarding their changes to privacy policies (for example, explaining the reasons behind the changes)
- consult with users on changes to the privacy policy
- provide adequate notice about changes to privacy policies explaining the exact nature of the changes prior to their roll out (in the form of emails or messages directly to members)
- provide choices regarding agreement to changes affecting personal information collected under earlier policies, such as options not to take up changes or new features.

5. That any changes to the retention and use of web browsing information are closely analysed for privacy impacts. In the Office's view, any collection and use of personal information for law enforcement purposes should be:
   - a necessary response to a clearly defined problem
   - proportionate to the risk posed
   - subject to a privacy impact assessment[9] and
   - accompanied by adequate accountability and review mechanisms.

[9] The Office has recently updated its guide on privacy impact assessments. The Office considers consultation and transparency to be important to the process. See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2010, www.privacy.gov.au/materials/types/download/9509/6590.

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth) (the Privacy Act), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses.

2. From 1 November 2010, the Office of the Privacy Commissioner will be replaced with a new statutory agency, the Office of the Australian Information Commissioner (OAIC). The OAIC will bring together the functions of privacy protection (including in the private sector), freedom of information (FOI) and information policy across the Australian Government.[10] The OAIC will be the national privacy regulator of the Privacy Act.

Introduction

3. The Office welcomes the opportunity to provide input to the Senate Standing Committee on Environment, Communications and the Arts (the Committee) inquiry into the adequacy of privacy protections for Australians online.[11]

4. Much of the information disseminated online is information about people – personal information – whether via blogs, social networks, online news sources, instant messaging, email, internet shopping and banking. In the internet age, information is easy to access and publish. It is searchable, downloadable, re-usable and can remain in circulation sometimes indefinitely.

5. These changed conditions for information handling can have a significant impact on the protection of individual privacy. Once released online, personal information can be difficult to recoup, delete or control. Despite the sheer scale of the internet, individual pieces of personal information can be located using increasingly powerful search engines and data analysis tools. Moreover, the value of personal information, for targeted marketing and other purposes, means

[10] Under the *Australian Information Commissioner Act 2010* (AIC Act, commencing 1 November 2010), the Office of the Privacy Commissioner will cease to exist and the Office of the Australian Information Commissioner (OAIC) will assume the regulatory functions under the *Privacy Act 1988*. The OAIC will have 3 statutory appointees: the Australian Information Commissioner as the CEO, the Privacy Commissioner and an FOI Commissioner. With the commencement of the AIC Act, references to the Office of the Privacy Commissioner will be deemed to be to the OAIC.

[11] Terms of reference for the inquiry are available at www.aph.gov.au/senate/committee/eca_ctte/online_privacy/index.htm.

that websites may be configured to elicit personal information rather than protect it.

6. The greater availability of personal information through online channels may also facilitate data aggregation and linking. When personal information from disparate sources is drawn together, it may allow conclusions to be drawn about an individual that they would prefer to keep private. Data aggregation may also enable new uses of personal information beyond the expectations of the individual and without their knowledge or consent.

7. In Australia, the Privacy Act provides a mechanism to support good personal information handling by government agencies and private sector organisations and offers an avenue of redress for individuals that believe that their personal information has been misused.

8. Since its enactment over twenty 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:

    - In March 2005 the Office released its Review of the Private Sector Provisions of the Privacy Act (the Private Sector Review), recommending the Government consider a wider review of privacy laws in Australia.[12]

    - In June 2005 a Senate Legal and Constitutional References Committee Inquiry recommended that the Government (through the Australian Law Reform Commission (ALRC)) undertake a comprehensive review of privacy regulation, including the Privacy Act.[13]

    - In January 2006 the ALRC received a reference from the then Australian Government. The ALRC's review of privacy from 2006 to 2008 included the release of Issues Papers 31 and 32, Discussion Paper 72, and extensive consultation, culminating in the release of its final report – *For your information: Australian Privacy Law and Practice* – in August 2008.[14]

[12] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988,* 2005, recommendation 1, www.privacy.gov.au/materials/types/reports/view/6049.

[13] Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988 (2005),* recommendations 1 and 2, www.aph.gov.au/Senate/committee/legcon_ctte/completed_inquiries/2004-07/privacy/report/index.htm.

[14] Australian Law Reform Commission, Issues Paper 31, 2006, *Review of Privacy* (ALRC IP 31); ALRC, Issues Paper 32, 2006, *Review of Privacy—Credit Reporting Provisions;* ALRC, Discussion Paper 72, 2007, *Review of Australian Privacy* (ALRC DP 72), *ALRC 108: For your information: Australian Privacy Law and Practice* (ALRC Report 108), 2008, paragraph 4.29, www.austlii.edu.au/au/other/alrc/publications/reports/108/.

- In October 2009 the Government announced its first stage response to Report 108, covering 197 of the 295 recommendations.[15]

- In June 2010, the Government released an exposure draft of the Australian Privacy Principles (APPs) which will replace the existing principles in the Privacy Act.[16] The APPs are a culmination of the reform work initiated by the ALRC in its review of privacy and carried forward by the Government in its response to that review.

9. The Office has been actively involved in the privacy law reform process since its Private Sector Review in 2005.[17] The Office made extensive submissions to ALRC Issues Papers 31 and 32 and Discussion Paper 72[18], has had informal input during the development of the draft APPs, and has made a detailed formal submission to the senate inquiry into the APPs.[19]

10. The Office is of the view that proposed reforms in line with the Government's response will enhance the operation of the Privacy Act, ensuring it remains effective in the face of continuing technological change. However, 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.

11. This submission is in two main parts. In **Part A** we discuss the importance of pursuing a multi-faceted approach to online privacy which combines principle-based legislation with user education, privacy enhancing technology and international cooperation on privacy law enforcement. In **Part B** we discuss a number of specific online privacy issues related to: social networking, privacy considerations for web 2.0, online behavioural advertising, use of web browsing information for law enforcement, converging technology and ubiquitous computing, and cloud computing.

[15] Australian Government, *First stage response to ALRC Privacy Report*, 2009 (Government Response 2009) www.dpmc.gov.au/privacy/reforms.cfm.

[16] *Australian Privacy Principles: Exposure draft* (APPs Exposure draft) www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/index.htm.

[17] Office of the Privacy Commissioner, *Getting in on the Act,* 2005.

[18] Office of the Privacy Commissioner, *Submissions to ALRC IP 32,* 2007 and *ALRC DP 72*, 2007.

[19] Office of the Privacy Commissioner, *Submission to Senate Finance and Public Administration Committee Inquiry into the Exposure Draft of the Australian Privacy Principles* (Submission to Exposure Draft of the APPs), August 2010.

Part A: Pursuing a multi-faceted approach to online privacy

12. The Office takes the view that the best approach to enhancing privacy online will be multi-faceted, comprising:

    i. principle-based legislation (with specific technology issues dealt with under binding codes where desirable and necessary)

    ii. end user empowerment through education

    iii. privacy enhancing technology design

    iv. international cooperation between jurisdictions.

i. Principle-based legislation and binding codes

Existing protections under the Privacy Act and proposals for reform

13. The Privacy Act regulates the handling of personal information by most Australian and ACT Government agencies, large private sector organisations and some small businesses. Agencies must comply with 11 Information Privacy Principles (IPPs) and organisations with ten National Privacy Principles (NPPs).

14. The IPPs and NPPs apply to personal information and set out standards for all aspects of the information lifecycle, from collection through use, disclosure and secure storage to (in the case of the NPPs) destruction or permanent de-identification. In the Privacy Act, personal information is defined as:

> ...information or an opinion [...], whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[20]

15. By taking the form of 'principles' rather than prescriptive rules, the standards in the Privacy Act seek to provide a framework adequately flexible to respond to technological change. For example, NPP 4.1 states that:

[20] *Privacy Act 1988*, s 6(1). The exposure draft for the APPs proposes a new definition for personal information which is: 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:
(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not.'
See *APPs Exposure draft,* cl 15.

> An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

'Reasonable steps' depend on the circumstances. For example, a particular level of encryption that provided adequate data security four years ago may no longer be sufficient due to technological advancement. In these circumstances, 'reasonable steps' may mean using more up-to-date encryption standards to protect the data. By setting out the desired outcomes rather than the technical standards, the principles allow the legislation to manage technological change.

16. One of the ALRC's major recommendations was for a continuation of principles-based approach to privacy regulation. It was the ALRC's view that 'principles allow for a greater degree of "future-proofing" and enable the regime to respond to new issues as they arise without having to create new rules.'[21] Moreover, the ALRC recommended that the two sets of principles in the Privacy Act (the IPPs and NPPs) be replaced by a single set of principles to reduce confusion, overlap and inconsistency.[22] As noted above, the Government accepted that recommendation and recently released an exposure draft of the new set of principles.[23]

17. The Office supports the continuation of principles-based regulation and the development of a single set of principles. We suggest that the Committee have regard to the Senate Finance and Public Administration Committee's inquiry into the exposure draft of the APPs in assessing the adequacy of privacy protections for online information handling, as well as the Office's submission to that inquiry.[24]

18. The Office believes that principle-based law continues to provide the best framework for privacy regulation in a changing technological environment.

Binding codes for emerging technologies

19. Currently, under the Privacy Act, organisations may voluntarily develop industry codes that are at least equivalent to the NPPs which organisations may consent to be bound by.[25]

---

[21] *ALRC Report 108*, 2008 paragraph 4.29.

[22] *ALRC Report 108*, 2008, recommendation 18-2.

[23] APPs *Exposure Draft*.

[24] Senate Finance and Public Administration Committee Inquiry into the Exposure Draft of Australian Privacy Principles, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm and Office of the Privacy Commissioner, *Submission the Exposure Draft of the APPs*, August 2010.

[25] *Privacy Act 1988*, s 18BB(2)(c).

20. The Government has committed to amending the Privacy Act to give the Privacy Commissioner the power to request the development of a privacy code by a defined group of organisations or agencies where the Commissioner believes a public interest would be served by the development of such a code.[26] The defined group of organisations or agencies could be either an industry sector or a group that engages in a particular practice (such as the use of a particular technology). The code would have to be approved by the Commissioner and, once in operation, would be mandatory for prescribed organisations or agencies.

21. The Government has further suggested that where an adequate code is not developed or approved following a formal request by the Privacy Commissioner, the Commissioner should have the power to develop and impose a binding privacy code on a defined group of organisations or agencies. This code making power would be accompanied by a requirement for consultation with relevant stakeholders similar to that currently required under the Privacy Act for Public Interest Determinations.[27]

22. 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. In the Office's submission to the ALRC's Discussion Paper 72, the Office noted that a binding code may be appropriate, for example, for certain types of data-matching where there may be heightened privacy risks[28], for specific notice requirements for new technologies[29], and to allow standards developed by industry bodies to be given lawful effect.[30]

23. 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. The Office believes that the proposed code-making power will enhance the responsiveness of the Act to technological change.

[26] Government Response, 2009, recommendation 48-1, page 89.

[27] Government Response, 2009, recommendation 48-1, page 89.

[28] Office of the Privacy Commissioner, *Submission to ALRC DP 72*, see proposal 7-6.

[29] Office of the Privacy Commissioner, *Submission to ALRC DP 72*, see proposal 7-5.

[30] Office of the Privacy Commissioner, *Submission to ALRC DP 72*, see proposal 7-2.

Areas outside the coverage of the Privacy Act

Small businesses

24. Most small businesses (those with an annual turnover $3 million or less) are not covered by the Privacy Act unless an exception applies.[31] Some of these exceptions include businesses that trade in personal information or provide a health service. The Explanatory Memorandum to the legislation stated that the exemption was '...in accordance with Government policy to minimise compliance costs for small business.'[32] For this reason, it was 'intended that small business be exempt from the legislation unless there is a privacy risk.'[33]

25. The ALRC stated in its review that 'given the increasing use of technology by small businesses, the risk posed to privacy may not necessarily be low.'[34] Certainly the dominance of electronic information coupled with the mass circulatory power of the internet has expanded the capacity for businesses of any size to impinge on privacy.

26. In its submission to the ALRC's review of privacy, the Office suggested that small businesses in the telecommunications sector that handle large amounts of personal information (such as internet service providers and public number directory producers) be brought in under the coverage of the Privacy Act.[35]

27. In its final report, the ALRC recommended the removal of the small business exemption all together.[36] Its view was that the exemption would become increasingly complicated as new small business sectors were brought in under the coverage of the Privacy Act. The Government has stated it will address the ALRC's recommendations regarding exemptions in its second round of privacy reforms.[37]

Organisations outside Australia

28. Generally the Privacy Act will not apply to organisations incorporated in other countries. However, the Act may have effect outside Australia under s 5B if the

[31] The exceptions are listed at s 6D, *Privacy Act 1988*.

[32] Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*.

[33] Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*.

[34] ALRC Report 108, 2008, paragraph 39.143.

[35] Office of the Privacy Commissioner, *Submission ALRC IP 31,* 2007, see pp 175-6.

[36] ALRC Report 108, 2008, recommendation 39-1.

[37] Department of the Prime Minister and Cabinet, *Privacy Reforms*, www.dpmc.gov.au/privacy/reforms.cfm.

act or practice of an organisation relates to the personal information of an Australian citizen or permanent resident **and** the organisation is either:

- an Australian organisation or
- an organisation that carries on business in Australia **and** collects or holds the information in Australia.

29. The Explanatory Memorandum to the legislation stated that this limited extra-territorial application of the Privacy Act was

> to ensure that, as far as practicable and appropriate, the legislation will apply in an environment where organisations operate across national boundaries and may move information overseas to use and process it. This is also intended to ensure that the provisions of the legislation are not avoided simply by moving personal information overseas.[38]

30. In the online context, there can be some uncertainty as to how s 5B of the Privacy Act applies to personal information submitted via the internet by individuals in Australia to an overseas organisation. The issue is whether the information was collected or held in Australia or not. 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.

31. The exposure draft of the APPs contains changes to s 5B of the Privacy Act. However, the proposed changes, as currently drafted, may not resolve the issue of where online collection occurs. In its submission to the senate inquiry into the exposure draft of the APPs, the Office suggests that this aspect be clarified, perhaps by amending the clause to refer to information collected **from** rather than **in** Australia.[39]

32. The Office suggests that the Committee have regard to the Senate Finance and Public Administration Committee's inquiry into the exposure draft of the APPs, and in particular its consideration of the issue of extra-territorial operation of the Privacy Act.[40]

33. As well as s 5B, the Privacy Act contains a 'transborder data flow' principle. NPP 9 outlines the circumstances in which an organisation can transfer personal

[38] Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000.*

[39] Office of the Privacy Commissioner, *Submission to Exposure Draft of the APPs*, August 2010.

[40] Senate Finance and Public Administration Committee Inquiry into the Exposure Draft of Australian Privacy Principles, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm.

information it holds outside Australian. This principle is based on the restrictions on international transfers of personal information set out in the European Union Directive 95/46.[41]

34. In simple terms, NPP 9 prevents an organisation from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual's consent or in some other limited circumstances.[42]

35. The exposure draft of the APPs introduces the notion of 'accountability' to the transborder data flow principle and extends the coverage of the principle to agencies.[43] The proposed new principle will hold Australian organisations accountable for an overseas recipient's acts or practices in relation to personal information, unless an exception applies.[44] The Office broadly supports the introduction of a concept of accountability to the transborder data flow principle, though has made some comments in relation to the detail of the proposed principle in its submission to the APP inquiry.[45]

36. With regard to online data flows, the Companion Guide to the draft APPs indicates that it is not intended that the transborder data flow principle will apply when personal information is routed through servers that may be outside Australia.[46] The Office agrees with this view provided the personal information is not accessed by a third party during this process. In its submission to the APP inquiry, the Office suggested that the Companion Guide or other explanatory material should note that entities will need to take a risk management approach to ensure that personal information simply routed overseas is not accessed by third parties.[47] If the information is accessed by third parties, this will be a 'disclosure' subject to the transborder data flow principle (among others).

37. In some cases, the global nature of the internet makes it difficult to determine where information is being collected, by whom and for what purpose. The Office therefore acknowledges the importance of international agreements between jurisdictions to ensure adequate privacy protections are in place no matter where

[41] Office of the Privacy Commissioner, *Guidelines to the National Privacy Principles*, 2001, p 58, www.privacy.gov.au/materials/types/guidelines/view/6582.

[42] *Privacy Act 1988,* see NPP 9.

[43] In the APPs, this principle has been renamed 'Cross-border disclosure of personal information'. For simplicity in this submission, we continue to refer to it as 'the transborder data flow principle'.

[44] See Australian Government, *Companion Guide to the Australian Privacy Principles* (APP Companion Guide), June 2010, p 13, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/guide/companion_guide.pdf.

[45] Office of the Privacy Commissioner, *Submission to Exposure Draft of the APPs*, August 2010.

[46] See *APP Companion Guide*, 2010, p 12.

[47] Office of the Privacy Commissioner, *Submission to Exposure Draft of the APPs*, August 2010.

organisations collect personal information. International cooperation on privacy enforcement is discussed below, paragraphs 52-59.

Individuals acting in a personal capacity

38. Generally, the IPPs and NPPs do not cover the actions of individuals acting in a personal capacity.[48] So, while an agency or organisation operating in Australia and collecting or disseminating personal information via the internet will be covered by the Act, an individual doing the same will not.

39. As we noted in our first submission to the ALRC's review of privacy, the internet allows for the wide circulation of information by an individual with little recourse for another individual impacted by the online publication of that information.[49] This is particularly the case with the new generation of web 2.0 tools, like blogs and wikis, which make it easy for ordinary internet-users to publish content.

40. In its review of privacy, the ALRC assessed options for 'take-down notices' for online content. Currently the *Broadcasting Services Act 1992* allows the Australian Communications and Media Authority to investigate complaints about content available via the internet and direct an internet content host to remove 'prohibited content'.[50] However, this take-down scheme does not cover information online that constitutes an invasion of privacy and the ALRC said:

> A take-down notice scheme would require a decision maker to balance the right of freedom of expression and the right to individual privacy. In the ALRC's view, it is more appropriate for a court, rather than a regulator, to undertake such a balancing act.[51]

41. The ALRC recommended the development of a statutory cause of action for privacy.[52] Such a cause of action may provide an avenue to redress a serious privacy invasion, including by individuals acting in a personal capacity. However, as the ALRC noted in its report:

> The ALRC is mindful that the implementation of the statutory cause of action for a serious invasion of privacy, recommended in this Inquiry, will not address entirely the inherent difficulties in regulating the use and disclosure of personal information

[48] See s 16E, *Privacy Act 1988*, noting however that in limited circumstances tax file number and credit reporting provisions in the Act may apply to individuals.

[49] See Office of the Privacy Commissioner, *Submission to ALRC IP 31*, chapter 11, paragraphs 49-54.

[50] ALRC Report 108, 2008, paragraph 11.10.

[51] ALRC Report 108, 2008, paragraph 11.23.

[52] ALRC Report 108, 2008, recommendations 74-1, 74-2, 74-3, 74-4 and 74-5.

> published on the internet. For example, while the Privacy Act has extraterritorial application, enforcing an order made by an Australian court in an action for serious invasion of privacy against a website hosted overseas may be difficult. In addition, information posted online can be copied onto an infinite number of other websites within seconds. It may be time consuming and costly—if not impossible—to remove altogether privacy invasive information from the internet.[53]

42. For this reason, the ALRC notes the importance of educating individuals as to the privacy impacts of posting personal information (including personal information of others) online. The Office agrees that end user education will be important and we discuss this further below at paragraphs 43-47.

ii. User empowerment through education

43. User-education will be critical to ensuring that individuals are equipped to protect their privacy online. Many aspects of online privacy remain in the hands of the individual including:

- how individuals choose to upload information
- the type of personal information they upload
- the steps they take to protect personal information online
- their confidence and familiarity with terms and conditions of use of online forums and social media
- their ability to effectively assess privacy consequences of certain online activities and to regulate behaviour accordingly.

44. Under s 27 (1)(m), the Privacy Commissioner is empowered to undertake educational programs for the purpose of promoting the protection of individual privacy. The ALRC recommended in its review that the Office develop guidance material on technologies that impact on privacy.[54] The Government supports this recommendation.[55]

45. The Office has set out in detail its cyber safety educational material in its recent submission to the Joint Select Committee on Cyber Safety.[56] Some examples

[53] ALRC Report 108, 2008, paragraph 11.24 (citations omitted).

[54] ALRC Report 108, 2008, recommendation 10-3.

[55] Government Response, 2009, recommendation 10-3, p 31.

[56] Office of the Privacy Commissioner *Submission to Joint Select Committee on Cyber Safety*, July 2010, www.aph.gov.au/house/committee/jscc/subs/sub_92.pdf.

include: the Office's youth portal and youth magazine which cover internet privacy issues faced by young people; FAQs on social networking and spam; and guidance on privacy and smartphones.[57] For organisations and agencies, the Office has developed guidance on responding to information security breaches and recently released a revised version of its *Privacy Impact Assessment Guide*.[58] In the Office's view, privacy impact assessments (PIAs) play an important role in ensuring that organisations and agencies have assessed and minimised the privacy impacts of new initiatives, including those involving the use of information and communication technology (ICT).

46. In its submission to the Joint Select Committee on Cyber Safety, the Office said that cyber safety is a national issue that requires a coordinated approach across portfolios and jurisdictions. It is the Office's view that privacy be treated as a separate topic within broader cyber safety education activities and not bundled with other concepts.[59]

47. The Office recommends that the Committee considers the work of the Australian Parliament Joint Select Committee looking into Cyber-safety as part of this inquiry.[60]

iii. Privacy enhancing technology

48. Along with legal frameworks and user education, technology itself can play an important role in fostering privacy friendly information handling. Digital technologies can be configured to allow individuals to remain anonymous or use a pseudonym, to limit the amount of personal information collected, to obtain and manage consent, to limit the scope for unintended secondary uses of personal information, to provide individuals with greater choice in relation to their personal information, to detect privacy settings and so on. These are commonly referred to as privacy enhancing technologies (PETs).

49. It is the view of the Office that when privacy is 'designed into' new systems at a formative stage, those systems are more likely to protect and manage personal information effectively. Other jurisdictions have explored options for promoting

[57] Office of the Privacy Commissioner: *Youth portal* www.privacy.gov.au/topics/youth; *FAQs on social networking* www.privacy.gov.au/faq/individuals#social_networking; *FAQs on spam* www.privacy.gov.au/faq/individuals#spam; *Mobilise your phone privacy* www.privacy.gov.au/topics/technologies.

[58] Office of the Privacy Commissioner: *Guide to Handling Information Security Breaches*, 2008, www.privacy.gov.au/materials/types/guidelines/view/6478; *Privacy Impact Assessment Guide*, (revised) 2010, www.privacy.gov.au/materials/types/download/9509/6590.

[59] Office of the Privacy Commissioner, *Submission to Joint Select Committee on Cyber Safety*, July 2010, p2.

[60] Joint Select Committee on Cyber-safety, www.aph.gov.au/house/committee/jscc/.

PETs. Notable examples include the UK Information Commissioner who released a report called *Privacy by design* in 2008 and the Information and Privacy Commissioner of Ontario who has released a number of reports and discussion papers on privacy and technology, including *Privacy by design: The Seven Foundational Principles* in 2009.[61]

50. The Office recommends that development and greater use of privacy enhancing technologies (PETs) be promoted with the aim of achieving the following outcomes:

    - ongoing research into, and development of, PETs
    - greater awareness amongst agencies and organisations as to the existence and desirability of PETs for personal information handling and
    - greater range and availability of PETs (including in off-the-shelf products).

51. The Office notes that the Canadian Office of the Privacy Commissioner allocates funding each year for non-profit research into privacy, including research into privacy information technology. Since the establishment of the contribution program in 2004, the Canadian Privacy Commissioner has allocated close to $2 million to more than 50 initiatives.[62]

iv. International cooperation between jurisdictions

52. Regulating online privacy 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 recognition of this fact, there has recently been considerable work done to strengthen international cooperation on privacy regulation.

53. The Asia Pacific Economic Cooperation (APEC) has developed a Privacy Framework aimed at '...encouraging the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific

[61] Information Commissioner's Office, *Privacy by design*, 2008, www.ico.gov.uk/upload/documents/pdb_report_html/html/1-foreword.html and Information and Privacy Commissioner of Ontario, see www.privacybydesign.ca/.

[62] Office of the Privacy Commissioner, Canada, news release, 'Canada's Privacy Commissioner Awards $454,000 for privacy research and awareness', 29 May 2009, www.priv.gc.ca/media/nr-c/2009/nr-c_090529_cp_e.cfm.

region'.[63] Since the Framework was endorsed by Ministers in 2004, the APEC Data Privacy Subgroup has been working on a pathfinder for implementation.

54. The APEC privacy pathfinder recently resulted in the development of a multi-lateral cross-border privacy enforcement arrangement for privacy enforcement authorities.[64] The arrangement, which commenced on 16 July 2010, seeks to facilitate cross-border enforcement of privacy law.[65] The Office is a co-administrator of the arrangement, and Australia was closely involved in the arrangement's development.[66]

55. The Organisation for Economic Cooperation and Development (OECD) has also undertaken work to foster international privacy standards and cooperation via its Working Party on Information Security and Privacy (WPISP).[67] The OECD's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* have provided the model for many privacy laws, including Australia's. In October 2006, WPISP released its report on *Cross-border enforcement of privacy laws* and in 2008 Ministers endorsed the *Seoul Declaration for the Future of the Internet Economy*[68]

56. In June 2007, OECD member governments adopted a recommendation for member countries to foster the establishment of an informal network of privacy enforcement authorities. In line with this recommendation, and consistent with relevant initiatives in other international forums (including APEC), 2010 marked the establishment of the Global Privacy Enforcement Network (GPEN).

57. The GPEN receives secretariat support from the OECD, including assistance with the development of a public website and a restricted access website for use by privacy enforcement authorities (currently under construction). The Office is one of the founding members of the GPEN. The inaugural meeting of the GPEN, held in Paris in March 2010, was attended by representatives from 12 privacy enforcement authorities.

---

[63] APEC Privacy Framework, paragraph 4, www.dpmc.gov.au/privacy/apec/apec_privacy_framework.cfm.

[64] APEC Cross-border Privacy Enforcement Arrangement, www.apec.org/apec/news___media/fact_sheets/201006cpea.html.

[65] The arrangement establishes a process under which participating authorities may contact each other for help with collecting evidence, sharing information on an organisation or matter being investigated, enforcing actions, and transferring complaints to another jurisdiction. The arrangement does not create legal obligations and assistance is limited to the existing jurisdiction and powers of the authorities involved. For further information see, www.apec.org/apec/news___media/fact_sheets/201006cpea.html.

[66] Special Minister of State, Media Release, *APEC Arrangement on International Privacy Enforcement*, www.smos.gov.au/media/2010/mr_392010.html.

[67] OECD Working Party on Information Security and Privacy, www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html.

[68] OECD Seoul Declaration, www.privacy.gov.au/aboutus/international/oecd.

58. Along with the privacy activities of APEC and OECD, the Office continues to foster strong ties with other privacy authorities in the region via the Asia Pacific Privacy Authorities group, of which the Office is a founding member.[69]

59. The Office notes the importance of Australia's ongoing participation in international forums to foster cooperation on privacy protection online.

Part B: Specific online privacy issues

i. Social networking

60. Online social networking has introduced a new form of human interaction that has changed the way many of us think about our privacy. Social networking makes it simpler to publish personal information and make it available to others. While social networks may have allowed people to reveal more about themselves than in the past, it does not follow that individuals no longer want or value privacy.

61. Privacy is sometimes associated with self-concealment. In the social networking context, it is more useful and realistic to conceive of privacy as being about individuals having a reasonable amount of control over their personal information. Sometimes social networking sites can impinge on individual privacy because they potentially remove some of that control. Individuals may lose control of their information because they have not adequately understood how to adjust their privacy settings or they publish information widely that they later wish to recoup. Individuals may also lose control when social networks change privacy settings or policies.

62. Generally it is up to individual users of social networking sites to make choices about their privacy that are right for them. Individuals will best be able to do this when they understand their privacy options and are informed as to the consequences of their behaviour online. However, social networks also have a role to play in implementing tools and policies that foster good personal information handling.

'Locative' social networking

63. 'Locative' social networking sites allow individuals to share their location with others. Generally locative social networking is associated with mobile devices such as smart phones. Users can use in-built GPS capabilities to capture and

[69] Asia Pacific Privacy Authorities, www.privacy.gov.au/aboutus/international/appa.

broadcast their location at a given moment. Some common examples of locative applications include Foursquare, Google Latitude, Loopt and Plancast. A few of these applications also work in conjunction with other social networks so a person's information shared using Foursquare, for example, will also be broadcast via Twitter.

64. The privacy issues associated with locative social media relate to the way it allows individuals to be located in real life. Some risks include that an individual inadvertently reveals a visit to a location that they would prefer to keep private. Sometimes individuals may be unaware of how widely their location has been broadcast or may configure their settings to be open, allowing people they don't know or don't know well to locate them. As with social networking generally, privacy risks can be mitigated by users being educated about online privacy and knowing how to use privacy settings.

Changes to social network privacy policies

65. Social networking privacy policies often contain a clause allowing the site to amend the policy at any time. Members of the networks are not sent an email about changes and must check the privacy policy on a regular basis to determine whether any changes have been made.[70] Generally there is no way for users of these sites to withhold their consent for changes to the handling of their personal information other than discontinuing their use of the site.

66. In other sectors, it may be reasonable and common for individuals to take their business elsewhere if they are unhappy with an organisation's privacy practices. However, in the social networking sector, individuals may be less inclined to change networks because this may mean leaving behind a network of friends that continue to use the site. For this reason, the Office believes that there is extra onus on social networking sites to be transparent as to privacy policy changes and to provide individuals with real choices with regard to the handling of their personal information.

67. In particular, social networking sites should:

- carry out a privacy impact assessment[71]

[70] Along with posting an updated policy on their privacy policy page, Facebook also publish changes to their Facebook Site Governance Page and users can elect to become a 'fan' of this page and receive notice of changes directly.

[71] See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2010, www.privacy.gov.au/materials/types/download/9509/6590.

- be transparent regarding their changes to privacy policies (for example, explaining the reasons behind the changes)
- consult with users on changes to the privacy policy
- provide adequate notice about changes to privacy policies explaining the exact nature of the changes prior to their roll out (in the form of emails or messages directly to members)
- provide choices regarding agreement to changes affecting personal information collected under earlier policies, such as options not to take up changes or new features.

68. The Office suggests that it assess options to provide guidance on these and other privacy-related matters to ensure that social networking sites are equipped to mitigate privacy risks for users.

Other channels for communicating privacy information

69. Under the Privacy Act, organisations must provide a notice to individuals when they collect their information, explaining (amongst other things) the purpose of the collection, the other organisations they are likely to disclose the information to, and the identity and contact details of the organisation.[72] Notice requirements help to make sure that individuals are aware of how their information is being handled and can maintain control over their privacy.

70. The Office understands that some people, particularly young people, who use social networking sites do not read privacy policies and for this reason, real-time privacy notices are particularly important. Research carried out by Australia Communications and Media Authority (ACMA) about young Australians' use of online social media reveals that:

> Children and young people have no desire to click on these links [to privacy policies and terms and conditions] and read the information available as they feel it will not tell them anything they do not already know, as well as often being very text heavy with lots of adult and legal wording. This results in safety messages being largely ignored or missed on social networking services.[73]

[72] *Privacy Act 1988*, NPP 1.3.

[73] Australian Communications and Media Authority, *Click and connect: Young Australians' use of online social media – Qualitative Research Report*, July 2009, page 68.

71. Some websites, like Facebook and Bebo, provide explanatory material in the form of FAQs[74] or short clips.[75] However, generally this material along with the privacy policy is only an optional link rather than a screen that new or existing members must read.[76]

72. The Office suggests that it assess options to provide guidance to social networks on providing adequate privacy notices and encouraging transparency with regard to personal information handling. For example, it would be helpful for users of social networks to be given a pop up notice when they change their privacy settings, explaining how the change will affect access to their personal information and seeking confirmation for the change. We understand that currently on some networks users only receive a warning message when they place restrictions on their profile and not when they are removing restrictions.

Individuals uploading personal information to social networks

73. In recent years there have been a number of reports of individuals posting information about themselves to social networks that they later regret.[77] Sometimes information has resulted in the person losing their job or having their party gatecrashed by uninvited guests.[78] On other occasions, posted information has led to embarrassment when the information is circulated more widely than intended, or when, down the track, individuals wish to distance themselves from past actions, beliefs or behaviours. On rare occasions, information posted on social networks may allow people to be tracked down in real life and harmed.[79]

74. The Office believes that user education is important to ensure individuals feel confident using social networking privacy controls and understand the consequences of uploading certain types of personal information online (also discussed above at paragraphs 43-47). Moreover, the Office notes the importance of clear privacy notices (discussed above at paragraphs 69-72) to ensuring that individuals are able to make informed decisions about their privacy.

[74] Facebook provides privacy FAQs and an easy to understand explanation of privacy settings: www.facebook.com/help/?topic=privacyupdate, www.facebook.com/privacy/explanation.php.

[75] Bebo safety portal contains a number of easy to understand clips and links: www.bebo.com/Safety.jsp.

[76] Australian Communications and Media Authority, *Click and connect,* 2009, page 69.

[77] See Jeffrey Rosen, 'The persistent memory', *The Age*, 31 July 2010.

[78] 'Mass brawl as 500 youths crash Facebook party', The Telegraph, 31 December 2008, www.telegraph.co.uk/news/uknews/4045928/Mass-brawl-as-500-youths-gatecrash-Facebook-party.html

[79] For example: 'Man accused of Facebook murder in court', *ABC News*, 28 July 2010, www.abc.net.au/news/stories/2010/07/28/2966467.htm.

ii. Privacy considerations for web 2.0 generally

User generated content

75. Many of the privacy issues raised in relation to social networking apply to web 2.0 tools more broadly. Web 2.0 is often characterised by enabling greater online interaction and user-generated content. Common web 2.0 tools include blogs, wikis and information sharing sites like Flickr and YouTube, which enable people, without specialised IT training, to publish information, comments and images online.

76. As with social networks, it is important that people consider privacy when posting information to blogs and wikis. Once information has been uploaded it can be difficult to recoup or delete. A particular privacy risk is that individuals expose the personal information of someone else in the course of using web 2.0 sites. This could inadvertently impinge on the privacy of a third party, or it may be an intentional action aimed at causing hurt or humiliation. Privacy risks can often be mitigated by responsive moderation.[80] Good outcomes will also be achieved where users are educated as to the importance of privacy online and what is appropriate in terms of the publication of personal information of others.

Digital identity management and anonymity

77. Digital identity management or IdM refers to the creation, verification, storage and use of digital identities over the internet. For some transactions online, organisations and agencies need to collect certain identity information to check that the individual is who they say they are.

78. With numerous online forums, services and portals requiring some form of identification of users, it is important that organisations and agencies are equipped to implement privacy friendly identity management systems.

79. Good identity management will allow identification of an individual only to the extent necessary for the transaction. Poor identity management will be overly and unnecessarily intrusive to the individual, minimise the individual's control over their personal information and possibly facilitate identity theft.

80. Some identity management issues associated with online transactions are:

[80] Moderation refers to the active monitoring of online forums and the removal of inappropriate content (such as privacy invasive information). Moderation can be done either by the site operator or by site users.

- the difficulty for individuals to determine the legitimacy and good intentions of an organisation collecting their personal information online
- the possibility of hackers and identity thieves inappropriately accessing personal information while it is being transmitted or once stored
- the emerging importance of measures, such as digital certificates and public key infrastructure, to authenticate the identity of an individual to enhance security (for example, in the place of a written signature)
- how individuals may interact anonymously in online environments, yet in a way that ensures that organisations and agencies have adequate information to conduct the transaction
- how to recognise that individuals may have multiple elements to their identity, depending on, for example, whether they are acting as a customer, an employee or a member of a family and that any online transaction need only authenticate the legitimacy of such identities to the extent necessary to enable the particular interaction
- the enhanced capacity to link personal information with other information already held or collected by electronic means.[81]

81. In the Office's view, good identity security means avoiding unnecessary collection of personal information. This is consistent with existing principles in the Privacy Act (and the draft APPs) which state that organisations and agencies should only collect personal information necessary for their functions or activities.[82] Authentication of an individual's identity, or any other characteristics of the individual, should only be conducted where necessary. The necessity of authentication may be determined by such factors as the risks associated with a given transaction or interaction. If the collection of information is for marketing purposes, the individual should be made aware of this and have an option of not providing their personal details.[83]

82. In the social networking context, there is a push towards greater sharing of authentication information between affiliated websites. In a recent paper developed by the OECD WPISP, it was noted that sharing of authentication

[81] Office of the Privacy Commissioner, *Submission to Department of Broadband, Communications and the Digital Economy: Digital Economy Future Directions*, February 2009, paragraph 56, www.privacy.gov.au/materials/types/download/8917/6687.

[82] *Privacy Act 1988,* see IPP 1 and NPP 1.1. See also, *APP Exposure draft,* draft APP 3.

[83] Office of the Privacy Commissioner, *Submission to Digital Economy Future Directions*, February 2009, paragraph 58.

information '... could make it easier for individuals to bring aspects of their social networking profiles to their activities at affiliated sites and in turn to have information about those activities exported back to their social networks'.[84] In these circumstances, the WPISP observed that '[e]nsuring the individual's privacy preferences are exchanged between organisations along with the personal data is important, along with sufficient transparency and accountability to facilitate effective user control'.[85]

83. Furthermore, online privacy risks can be greatly reduced when individuals are allowed to remain anonymous. Currently the Privacy Act requires organisations to provide individuals with the option of not identifying themselves when interacting with the organisation, where this is lawful and practicable.[86] The current draft APPs will extend this requirement to agencies. The draft APPs also provide for the use of pseudonyms by individuals in certain circumstances.[87]

84. The Office supports the development of privacy friendly digital identity management systems, including those that enable the individual to use a pseudonym. Generally, privacy protection will be most effective in identity management systems where it is built in at the beginning. In its review of privacy, the ALRC made recommendations that the Office develop guidance material on various aspects of anonymity and pseudonymity and on privacy and technology more generally and the Government has responded favourably to these recommendations.[88] The Office will seek to issue guidance on anonymity and pseudonymity following the finalisation of the new APPs.

De-identification of personal information

85. In 2009, the Government established the Government 2.0 Taskforce (the Taskforce) to investigate how the public sector could make better use of web 2.0 tools and approaches.[89] The Taskforce addressed options for enhancing the use of government information and encouraging greater collaboration between agencies

[84] OECD Working Party on Information Security and Privacy, *The role of digital identity management in the internet economy: A primer for policy makers*, 11 June 2009, p 9, www.oecd.org/dataoecd/55/48/43091476.pdf.

[85] OECD Working Party on Information Security and Privacy, *The role of digital identity management in the internet economy*, 11 June 2009, p 9.

[86] *Privacy Act 1988,* see NPP 8.

[87] See ALRC Report 108, 2008, chapter 20; Government Response 2009, recommendation 20-1, p 39; *APP Exposure Draft*, Draft APP 3.

[88] ALRC Report 108, 2008, see recommendations 20-2 and 10-2.

[89] Government 2.0 Taskforce, gov2.net.au/.

and the public. Its final report was delivered in December 2009.[90] The Government responded to the Taskforce's report in May 2010.[91]

86. The Taskforce made recommendations in relation to government information which may include personal information.[92] A major theme of the Taskforce's final report was that government information should be treated as a national resource and as such should be made available as much as possible. In releasing data-sets, agencies allow others to mash, re-work, re-focus, combine and otherwise add value to existing data.

87. Under the Privacy Act, personal information may not be disclosed other than for the purpose it was collected unless an exception applies. However there are no restrictions on disclosure of de-identified information as long as the identity of the individual is not apparent or 'reasonably ascertainable'.[93]

88. As data analysis and linkage technology becomes more sophisticated, risks of re-identification may be greater, particularly given the growing availability of personal information online from a range of sources. Both the Government 2.0 Taskforce and the Australian Law Reform Commission have made recommendations that the Office publish guidance material on de-identification of personal information.[94] The Office agrees that guidance on de-identification is desirable and will be assessing options for the development of such guidance.

iii. Online behavioural advertising

89. Online behavioural advertising involves the collection of data from a computer or web browser about web-viewing behaviours over time and across sites in order to predict user preferences and interests and deliver targeted advertising based on these interests.

90. This data can be collected in a number of ways but typically involves websites or advertising companies placing a 'cookie' on a browser. This enables advertisers to track the sites visited by that browser and thus build up a picture of the users'

[90] Government 2.0 Taskforce, *Engage: Getting on with Government 2.0: Report of the Government 2.0 Taskforce,* www.finance.gov.au/publications/gov20taskforcereport/index.html.

[91] Australian Government, *Government Response to the Report of the Government 2.0 Taskforce*, www.finance.gov.au/publications/govresponse20report/index.html.

[92] Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*.

[93] The *Privacy Act 1988* applies to 'personal information' which is defined in the Act as: '...information or an opinion [...], whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion', see *Privacy Act 1988,* s 6(1). The definition of personal information is referred to above at paragraphs 14.

[94] See Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*, recommendation 11, and ALRC Report 108, 2008, recommendations 6-3 and 28-5.

interests and habits. This information is then used to display advertisements that target these interests. The ads displayed may relate to general interest categories or directly advertise previously-visited websites.[95]

91. Providers of online behavioural advertising say that only information from the browser is collected and that this in itself cannot identify an individual.[96] As such, the data collected may not be personal information as defined by the Privacy Act. 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.[97]

92. Online behavioural advertising raises many of the same issues for consumers as direct marketing as it involves targeting advertising based on past behaviours. Currently, NPP 2 allows the use of personal information for direct marketing if certain conditions are met. NPP 2 distinguishes between information collected for the purpose of direct marketing (primary purpose) and that collected for another purpose but then used for direct marketing (secondary purpose).

93. The ALRC recommended that a discrete privacy principle regarding direct marketing be developed that would remove this distinction and instead distinguish between existing customers of an agency or organisation and new ones.[98] Draft APP 7 sets out to distinguish between 'individuals who have provided personal information to the entity who is undertaking the direct marketing' and 'those who have not provided personal information to the entity who is undertaking the direct marketing'.[99] However, this principle will not apply to online behavioural advertising if the information gathered is not personal information.

94. As noted in paragraphs 43-47, it is important that users are informed about the implications of their actions online and the sorts of information they may be giving away about themselves. The Office supports measures that assist individuals to make informed and meaningful choices about their online activities. In this context, individuals should be informed when their browsing information is being collected, the purposes for which it may be used, whether it

[95] Google Ads Preferences FAQs www.google.com/ads/preferences/html/faq.html#advertisers .

[96] Your Online Choices: A guide to online behavioural advertising www.youronlinechoices.com/what-is-behavioural-advertising (accessed 17 August 2010).

[97] M Barbaro and T Zeller, 'A Face is Exposed for AOL Searcher No. 4417749', *New York Times*, 6 August 2006 query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63.

[98] ALRC Report 108, 2008, recommendation 26-1.

[99] *APP Companion Guide*, 2010, p 11.

may be disclosed to other organisations or aggregated with other information, and how to opt out of having it collected.

iv. Use of web browsing information for law enforcement

95. The Office acknowledges that information about the online activities of individuals may, in certain circumstances, be useful to the investigations of law enforcement agencies. However, broad scale collection and retention of web browsing information could significantly impact on the privacy of individuals. Possible privacy issues could include greater risks of data loss or misuse, unwarranted surveillance, data linking and data mining, and identity theft.

96. It is important that any changes to the retention and use of web browsing information are closely analysed for privacy impacts. In the Office's view, any collection and use of personal information for law enforcement purposes should be:

- a necessary response to a clearly defined problem
- proportionate to the risk posed
- subject to a privacy impact assessment[100] and
- accompanied by adequate accountability and review mechanisms.

v. Converging technology and ubiquitous computing

97. As technologies converge, it is likely that collection, use, disclosure and transfer of data will become increasingly seamless. This is particularly the case with ubiquitous computing or 'the internet of things'.[101] Seamless data collection, collation and transfer may create challenges for ensuring that individuals have a measure of control over how their information is used and disclosed. It may also

[100] The Office has recently updated its guide on privacy impact assessments. The Office considers consultation and transparency to be important to the process. See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2010, www.privacy.gov.au/materials/types/download/9509/6590.

[101] Wikipedia describes ubiquitous computing as: '...a post desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities. [...]For example, a domestic ubiquitous computing environment might interconnect lighting and environmental controls with personal biometric monitors woven into clothing so that illumination and heating conditions in a room might be modulated, continuously and imperceptibly. Another common scenario posits refrigerators "aware" of their suitably-tagged contents, able to both plan a variety of menus from the food actually on hand, and warn users of stale or spoiled food.' (Accessed on 13 August 2010), en.wikipedia.org/wiki/Ubiquitous_computing.

mean that traditional methods of providing privacy notices are difficult to achieve.

98. Related to ubiquitous computing is the development of smart infrastructure systems such as the smart grid and smart transport systems. Some have predicted that the amount of data generated by smart grids will be far greater than the internet.[102]

99. Smart infrastructure will generate information about the behaviours of individuals. For example, smart meters and smart appliances can reveal detailed information about what is occurring at a residence at any one moment. The Ontario Information and Privacy Commissioner says that the raw data from smart meters and smart appliances could reveal:

> Whether individuals tend to cook microwavable meals or meals on the stove; whether they have a cooked breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used.[103]

100. The risk with a rich, new data source is the temptation to use the information for more than originally intended. Data collected about a person's electricity usage for billing and efficiency suggestions could be desirable to appliance vendors. There are many parties that may have an interest in this sort of data, from manufacturers wanting to know how their products are used to burglars looking for the ideal time to break into a property.

101. Where information identifies an individual – for example, where smart infrastructure data is connected with the address and billing details of an individual – the information is personal information and the Privacy Act will apply. This means that organisations or agencies delivering smart infrastructure will have to ensure that they provide individuals with notice which includes advice that the information is being collected. Organisations also may only use information for the purpose for which it was collected, must store the information securely, and must delete it when it is no longer needed for the purpose for which it was collected.

---

[102] Martin LaMonica,"Cisco: Smart grid will eclipse the size of the Internet", *CNET*, 18 May 2009, news.cnet.com/8301-11128_3-10241102-54.html.

[103] Information and Privacy Commissioner, Ontario, Canada, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, November 2009, p11.

102. Challenges to applying the Privacy Act may arise when information is associated with a household rather than an individual. The Privacy Act will not apply if the information does not qualify as 'personal information'. In these circumstances, it is important that specific privacy protections, including legislative protections, are established to ensure that smart infrastructure information is handled appropriately.

103. Currently the House Standing Committee on Infrastructure, Transport, Regional Development and Local Government is carrying out an inquiry into smart infrastructure.[104] The Office recommends that the Committee consider that inquiry for the purposes of its own inquiry into online privacy to ensure areas of mutual interest are consistently addressed.

vi. Cloud computing

104. Cloud computing allows organisations and agencies to leverage the massive computing power of the internet to meet data processing demands. By outsourcing data processing to cloud vendors, organisations and agencies can take advantage of almost limitless data storage through virtualisation and may reduce the amount spent on in-house IT systems.

105. 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.

106. A key issue is that due to virtualisation, personal information of Australians may end up being stored in data centres in other countries. Organisations may need to comply with the transborder data flow principle in the Privacy Act, depending on the nature of the relationship between the organisation and cloud vendor.[105] This may mean checking that data held overseas is governed by privacy law substantially similar to standards in the Privacy Act, or that cloud vendors are appropriately bound by contracts that require that adequate privacy standards are met.

107. The Office suggests that organisations and agencies undertake a PIA on changes to their data processing practices, including changes involving storage of data 'in the cloud'. Furthermore, the Office considers it would be good practice

[104] House of Representatives Standing Committee on Infrastructure, Transport, Regional Development and Local Government, Smart Infrastructure Inquiry, www.aph.gov.au/house/committee/itrdlg/smartinfrastructure/index.htm.

[105] See *Privacy Act 1988,* NPP 9. See also *APP Exposure Draft*, Draft APP 8.

for organisations and agencies to make it clear in their privacy policies and notices if personal information will be sent overseas. In this regard, the current draft APPs would require agencies and organisations to notify individuals if they are likely to disclose personal information to overseas recipients.[106] The Office supports this draft requirement as a means of ensuring that individuals have sufficient information about how their personal information may be handled.

vii. Privacy impact assessments for new online initiatives

108. The Office supports the use of PIAs by organisations and agencies to ensure that privacy is built into new online initiatives.

109. A PIA is an assessment tool that describes in detail the personal information flows in a project, and analyses the possible privacy impacts of the project.

110. The elements that make up a PIA (including identification, analysis and management of privacy risks) help organisations and agencies to develop and implement good privacy practice and underpin good public policy. PIAs also help to engender community trust in ICT proposals if the issues raised during the PIA are responded to adequately through the proposal's development.

111. Generally, a PIA should:

- describe the personal information flows in a project
- analyse the possible privacy impacts of those flows
- assess the impact the project as a whole may have on the privacy of individuals and
- explain how those impacts will be eliminated or minimised.

112. For large projects, conducting a PIA may be an iterative process, with a number of PIAs done at various stages of development or as project design evolves. In many cases it can be useful for PIAs to be conducted by an independent expert specialising in privacy issues and the process of conducting PIAs. There are many organisations equipped to undertake this role.[107]

[106] *APP Exposure draft,* Draft APP 5 (2)(i) and (j).

[107] See, for example: www.privacy.gov.au/aboutprivacy/helpme/psp. Note that privacy service providers listed at this link are not endorsed by the Office.

113. In its review of privacy, the ALRC recommended that the Privacy Commissioner be empowered to direct an agency to provide to the Commissioner a PIA in relation to a new project or development that may have a significant impact on the handling of personal information.[108] The Government accepted this recommendation.[109]

114. The ALRC also recommended that the Office develop and publish PIA guidelines tailored to the needs of private sector organisations.[110] The Office recently released a new version of its PIA guide that caters to the needs of both organisations and agencies in response to that recommendation.[111] Additionally, the ALRC said that five years after the commencement of the amended Privacy Act, a review should be undertaken to assess whether the power to direct an agency to undertake a PIA should be extended to private sector organisations.[112] The Government accepted this recommendation that later consideration be given to extending this power.[113]

[108] ALRC Report 108, 2008, recommendation 47-4.

[109] Government Response, 2009, recommendation 47-4, p 86.

[110] ALRC Report 108, 2008, recommendation 47-5.

[111] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2010, www.privacy.gov.au/materials/types/download/9509/6590.

[112] ALRC Report 108, 2008, recommendation 47-5, p 86.

[113] Government Response, 2009, recommendation 47-5, p 86-7.